(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－305512
（P2002－305512A）
(43)公開日　平成14年10月18日(2002.10.18)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｈ　1/00	Ｆ	５Ｊ１０４
Ｈ０４Ｈ　1/00		Ｈ０４Ｌ　9/00	６０１Ａ	
			６０１Ｄ	

審査請求　未請求　請求項の数29　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－91685(P2001－91685)
(22)出願日　平成13年３月28日(2001.3.28)
(31)優先権主張番号　特願2001－25011(P2001－25011)
(32)優先日　平成13年２月１日(2001.2.1)
(33)優先権主張国　日本（ＪＰ）

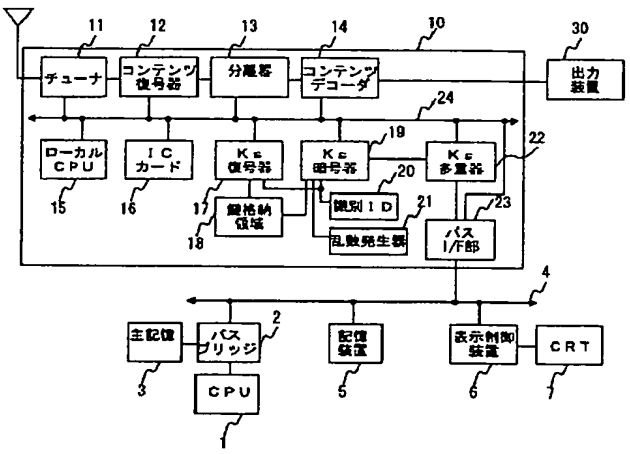
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　森野　東海
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　岡山　祐孝
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　データ受信装置

(57)【要約】
【課題】本発明の課題は、放送データを受信するデータ処理装置に於いて、ファイル操作を行うことができるアプリケーションが動作するＰＣなどのデータ処理装置に於いても、コンテンツデータの著作権の保護が可能でワーク鍵ｋｗが変更になってもコンテンツを視聴可能なデジタル放送データ転送処理装置を提供することにある。
【解決手段】本発明は、暗号化されたコンテンツと暗号化されたスクランブル鍵とを受信するチューナ１１と、ＩＣカード１６内のワーク鍵を用いて暗号化スクランブル鍵を復号化させるローカルＣＰＵ１５と、データ受信装置１０に固有の識別ＩＤと任意の乱数とに基づいて、復号化スクランブル鍵を再暗号化するための暗号鍵と、再暗号化スクランブル鍵を再復号化するための復号鍵とを生成し、暗号鍵を用いて復号化スクランブル鍵を再暗号化するＫｓ暗号器１７と、復号鍵を記憶する鍵格納領域１８と、再暗号化スクランブル鍵と暗号化コンテンツとを外部装置へ転送するバスＩ／Ｆ部２３とを備える。

【図１】



1

【特許請求の範囲】

【請求項１】暗号化されたデータであって、前記データが時間の経過により内容が変更されるデータ復号鍵により復号化するデータを受信するデータ受信装置において、以下の構成を有する、

第1の暗号鍵により暗号化された前記データを受信する受信器、および受信された前記データおよび第2の暗号鍵により暗号化された前記データ復号鍵の少なくとも一方を復号化する復号器と接続され、復号化された前記データまたは前記データ復号鍵を、再暗号化鍵により再暗号化する暗号器を有し、前記暗号器と接続され、再暗号化された前記データおよび再暗号化された前記データ復号鍵のうち少なくとも一方を、記憶媒体に記憶する。

【請求項２】請求項１に記載のデータ受信装置において、

さらに、前記暗号器と接続された多重化器を有し、前記復号器は、前記データ復号鍵を復号化し、

前記暗号器は、復号化された前記データ復号鍵を暗号化し、前記多重化器は、再暗号化された前記データ復号鍵と受信された前記データの対応付けを行い、前記対応付けられた再暗号化された前記データ復号鍵および前記データを、前記記憶媒体に記憶する。

【請求項３】請求項２に記載のデータ受信装置において、

前記暗号器は、当該暗号器で暗号化された前記データ復号鍵を復号する再復号鍵を生成し、再暗号化された前記データ復号鍵と前記復号鍵を互いに関連付けて第２の記憶媒体に記憶する。

【請求項４】請求項２に記載のデータ受信装置において、

さらに、前記受信器に接続された第１の分離器および第２の分離器を有し、前記受信器は、暗号化された前記データおよび暗号化された前記データ復号鍵を含む送信情報を受信し、前記第１の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データを復号化して表示装置に送信し、前記第2の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データ復号鍵を前記復号器に送信し、分離された前記データを前記多重器に送信する。

【請求項５】請求項２に記載のデータ受信装置において、前記暗号器は、当該データ受信装置を識別する識別情報に基づいて作成された前記再暗号化鍵を用いる。

【請求項６】請求項５に記載のデータ受信装置において、前記暗号器は、さらに乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いる。

【請求項７】請求項２に記載のデータ受信装置において、さらに、前記復号器を有する処理装置と接続するインターフェースユニットを有し、前記暗号器は、前記処理装置を識別する識別情報に基づいて作成された前記再

2

暗号化鍵を用いる。

【請求項８】請求項７に記載のデータ受信装置において、前記暗号器は、さらに乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いる。

【請求項９】請求項２に記載のデータ受信装置において、

当該データ受信装置は、前記記憶媒体をさらに有する。

【請求項１０】請求項２に記載のデータ受信装置において、

当該データ受信装置は、バスを介して前記記憶媒体と接続する。

【請求項１１】請求項２に記載のデータ受信装置において、

さらに、当該データ受信装置の利用者からの入力に応じて、前記暗号器で暗号化された前記データ復号鍵を復号化し、復号化された前記データ復号鍵を用いて前記記憶媒体に記憶された前記データを復号化する第2の復号器、および前記第2の復号器と接続され、復号化された前記データを出力する出力器を有する。

【請求項１２】請求項１に記載のデータ受信装置において、前記復号器は、受信された前記データを復号化し、

前記暗号器は、復号化された前記データを暗号化し、暗号化された前記データを復号するための第２の復号鍵を生成し、

前記暗号器で暗号化された前記データを前記記憶媒体に、前記第２の復号鍵を第２の記憶媒体に互いに関連付けて記憶する。

【請求項１３】請求項１２に記載のデータ受信装置において、

さらに、前記受信器に接続された第１の分離器および第２の分離器を有し、前記受信器は、暗号化された前記データおよび暗号化された前記データ復号鍵を含む送信情報を受信し、前記第１の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データを復号化して表示装置に送信し、前記第２の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データを前記復号器に送信する。

【請求項１４】請求項１２に記載のデータ受信装置において、前記暗号器は、当該データ受信装置を識別する識別情報に基づいて作成された前記再暗号化鍵を用いる。

【請求項１５】請求項１４に記載のデータ受信装置において、前記暗号器は、さらに乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いる。

【請求項１６】請求項１２に記載のデータ受信装置において、さらに、前記復号器を有する処理装置と接続するインターフェースユニットを有し、前記暗号器は、前記処理装置を識別する識別情報に基づいて作成された前記再暗号化鍵を用いる。

【請求項１７】請求項１６に記載のデータ受信装置にお

いて、前記暗号器は、さらに乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いる。

【請求項１８】請求項１２に記載のデータ受信装置において、

当該データ受信装置は、前記記憶媒体をさらに有する。

【請求項１９】請求項１２に記載のデータ受信装置において、

当該データ受信装置は、前記記憶媒体とバスを介して接続する。

【請求項２０】請求項１２に記載のデータ受信装置において、

前記第2の記憶媒体を有する第2の処理装置と接続する第2のインターフェースユニットを有する。

【請求項２１】請求項１２に記載のデータ受信装置において、

さらに、当該データ受信装置の利用者からの入力に応じて、前記第2の復号鍵を用いて前記記憶媒体に記憶された前記データを復号化する第2の復号器、および前記第2の復号器と接続され、復号化された前記データを出力する出力器を有する。

【請求項２２】請求項１に記載のデータ受信装置において、前記受信器は、放送局から放送される暗号化された前記データおよび所定周期ごとに内容が変更され、暗号化されたデータ復号鍵を含む放送情報を受信し、

【請求項２３】請求項１に記載のデータ受信装置において、

前記第1の暗号鍵は、前記第2の暗号鍵である。

【請求項２４】暗号化されたデータであって、前記データが時間の経過により内容が変更されるデータ復号鍵により復号化されるデータを再生するデータ再生装置において、以下の構成を有する、

記憶媒体から第1の暗号鍵で暗号化された前記データおよび第2の暗号鍵で暗号化された前記データ復号鍵を読み出す手段、

前記データ復号鍵を復号化する手段、復号された前記データ復号鍵を用いて、読み出されたデータを復号化する手段、および復号化された前記データを出力する手段。

【請求項２５】請求項３に記載のデータ受信装置において、さらに、

前記第２の記憶媒体を有する第２の処理装置と接続する第２のインターフェースユニットを有する。

【請求項２６】請求項２５に記載のデータ受信装置において、前記第２のインターフェースユニットは、暗号通信を用いて、前記第２の記憶媒体に格納される前記再復号鍵を送受信する。

【請求項２７】請求項２０に記載のデータ受信装置において、前記第２のインターフェースユニットは、暗号通信を用いて、前記第２の記憶媒体に格納される前記再復号鍵を送受信する。

【請求項２８】請求項１に記載のデータ受信装置において、

さらに、前記暗号器と接続され、１以上の鍵を記憶する鍵記憶媒体を有し、

前記暗号器は、前記鍵記憶媒体に記憶された鍵のうち少なくとも１つを用いて、復号化された前記データおよび復号化された前記データ復号鍵のうち少なくとも一方を再暗号化し、前記再暗号化に用いられた鍵と前記再暗号化された前記データおよび再暗号化された前記データ復号鍵のうち少なくとも一方を関連付け、前記再暗号化された前記データおよび再暗号化された前記データ復号鍵のうち少なくとも一方を、前記記憶媒体に格納する。

【請求項２９】請求項１に記載のデータ受信装置において、

前記暗号器は、少なくとも復号化された前記データを再暗号化する。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化されたコンテンツを受信するデータ受信装置及びそのデータ受信装置を有する情報処理装置に係わる。そのなかでも特にデジタル放送データやネットワークを介して伝送されたデータを受信するデータ受信装置及びそのデータ受信装置を有する情報処理装置に関する。なお、データ受信装置には、テレビ受像機（チューナ）、ビデオレコーダ、セットトップボックス等が含まれる。また、情報処理装置には、パーソナルコンピュータ、ワークステーション、携帯電話が含まれる。

【０００２】

【従来の技術】近年、衛星放送等を用いた電子配信により、暗号化された映像や音声コンテンツをユーザに提供するデータ配信が行われている。「ＢＳデジタル放送限定受信方式」ＡＲＩＢ・ＳＴＤ－Ｂ２５では、ＢＳデジタル放送における限定受信の方法が記述されている。図２に、この記述内容であるＢＳデジタル放送での暗号化されたデータを受信する限定受信方式を示す。

【０００３】この図２を用いてデータの流れを説明する。まず、映像や音声等のコンテンツはコンテンツ暗号器１０１でスクランブル鍵Ｋｓ１０２を用いて暗号化される。また、スクランブル鍵Ｋｓ１０２は暗号器１０６でワーク鍵１０３を用いて暗号化され、ワーク鍵Ｋｗ１０３と契約情報１０４は暗号器１０７でマスター鍵Ｋｍ１０５を用いて暗号化される。これら、暗号化されたコンテンツ、スクランブル鍵Ｋｓ及びワーク鍵Ｋｓと契約情報は多重器１０８で多重化され受信機に配信される。また、受信機１２０では分離器１１８を用いて暗号化されたコンテンツ、スクランブル鍵Ｋｓ及びワーク鍵Ｋｗと契約情報に分離される。暗号化されたワーク鍵Ｋｗと契約情報は復号器１１７でマスター鍵１１５を用いて復号されワーク鍵Ｋｗと契約情報１１４を得て保存する。暗号化されたスクランブル鍵は復号器１１６でワーク鍵

5

Ｋｗを用いて復号されスクランブル鍵Ｋｓを得る。また、暗号化されたコンテンツは、契約情報１１９を用いて視聴判定器１１９で視聴可能かどうかを判定し可能であればコンテンツ復号器１１１でスクランブル鍵Ｋｓを用いて復号化される。ここでスクランブル鍵Ｋｓは暗号化され全ての受信機で受信されるが、ワーク鍵Ｋｗと契約情報は受信機毎のデータであり受信機毎にユニークなマスター鍵Ｋｍで暗号化され他の受信機以外では復号化できない。したかって契約していないコンテンツは、スクランブル鍵Ｋｓを復号化するために必要なＫｗが得られないため受信できない事になる。マスター鍵Ｋｍは変更される事はないが、ワーク鍵Ｋｗは契約時とおよそ半年から１年程度で変更され、スクランブル鍵Ｋｓはおよそ数秒単位で更新される。このため契約していないコンテンツのワーク鍵Ｋｗが分かったとしても１年程度、スクランブル鍵Ｋｓが分かった場合は数秒程度しか視聴する事しかできなくなっている。また、図２の復号器１１６、復号器１１７、マスター鍵１１５、契約情報１１４、視聴判定器１１９はＩＣカードで実現されている。

【０００４】また、図３のようにパーソナルコンピュータ（ＰＣ）に接続可能なＢＳデジタル放送の受信ボードが存在する。

【０００５】

【発明が解決しようとする課題】コンテンツを録画する場合には、以下の問題が生じる。この問題を図3に示す場合を例に説明するが、その他、PCを含む情報処理装置内に受信ボードがある場合、テレビ受像機、セットトップボックス、ビデオレコーダの場合でも同様の問題が生じる。

【０００６】図３のようにＢＳデジタル放送の受信ボードをパーソナルコンピュータ（ＰＣ）に接続した場合に、ＰＣで録画機を実現すると次のようになる。チューナ１１で受信したデジタルデータは、分離器１３で暗号化されたスクランブル鍵Ｋｓ、ワーク鍵Ｋｗや契約情報を分離して、ローカルバス２４を介してローカルＣＰＵ１５によりＩＣカード１６に送られる。ＩＣカード１６では、上述したように、ワーク鍵Ｋｗや契約情報を保存し、暗号化されたスクランブル鍵Ｋｓを復号化する。そしてコンテンツ復号器１２にスクランブル鍵Ｋｓを送り、暗号化されたコンテンツを復号化する。復号化されたコンテンツはコンテンツデコーダ１４でデコードされモニタやスピーカなどの出力装置３０に出力される。このとき、出力装置３０ではなくＰＣの表示制御装置６に直接出力することも考えられる。また、ＰＣのＨＤＤの様な記憶装置５に録画するには、分離器１３で分離したコンテンツをローカルバス２４よりバスＩ／Ｆ部２３に送られ、ＰＣの内部バスであるＰＣＩバス４を介してバスブリッジ２を経由し主記憶３に格納される。主記憶３にある程度コンテンツが蓄積されるとＣＰＵ１により、記憶装置５に格納される。ここで、記憶装置５に格納さ

6

れたコンテンツは暗号化されておらず、ファイル操作を行うアプリケーションを用いると簡単にコピーができてしまい、コンテンツの著作権の保護が困難になる。

【０００７】また、コンテンツの著作権を保護するためにコンテンツやスクランブル鍵Ｋｓを暗号化されたまま、記憶装置５に格納し再生するときに暗号を復号する事が考えられるがこれは、上述したようにワーク鍵Ｋｗが半年から１年程度で変更されてしまうため録画してから時間が経つとコンテンツを視聴できなくなってしまうと言った問題がある。

【０００８】

【課題を解決するための手段】本発明の目的は、コンテンツの著作者等の権利の保護を図りつつ、視聴者側で適切な記憶媒体又は記憶装置でコンテンツを管理できるデータ受信装置及び情報処理装置を提供することである。

【０００９】この目的を達成するために、本発明は、暗号化されたデータであって、前記データが時間の経過により内容が変更されるデータ復号鍵により復号化するデータ対象とし、第1の暗号鍵により暗号化された前記データを受信し、受信された前記データおよび第2の暗号鍵により暗号化された前記データ復号鍵の少なくとも一方を復号化し、復号化された前記データまたは前記データ復号鍵を、再暗号化鍵により暗号化し、前記暗号器と接続され、暗号化された前記データまたは前記データ復号鍵を、記憶媒体に記憶する。

【００１０】また、本発明には、記憶媒体に記憶されたデータを再生することも含まれる。

【００１１】

【発明の実施の形態】次に本発明の実施例について図面を用いて詳細に説明する。図１は、本発明の１情報処理装置を示すブロック図である。図１において、１９はスクランブル鍵を再暗号化するＫｓ暗号器で、２０はデータ受信装置１０毎又は情報処理装置毎のユニークな識別情報である識別ＩＤ（Identifier）を格納する識別ＩＤ格納領域で、２１は乱数を発生させる乱数発生器で、１８はコンテンツのＩＤとＫｓ暗号器１９で暗号化されたスクランブル鍵を復号化する鍵を格納する鍵格納領域である。２２は再暗号化されたスクランブル鍵Ｋｓを暗号化されているコンテンツに多重化を行うＫｓ多重器である。１７は、再暗号化されたスクランブル鍵Ｋｓの復号を行う復号器である。

【００１２】情報処理装置は、データを受信し復号化及び再暗号化を行うデータ受信装置１０と、データを視聴するための出力装置３０と、情報処理を実行する情報処理装置本体と、表示を行うためのＣＲＴ（Cathode-Ray Tube）７とを備える。尚、ＣＲＴ７は、液晶ディスプレイ、プラズマディスプレイ、ＥＬディスプレイ等のデータを表示する他の表示装置であってもよい。

【００１３】情報処理装置本体は、演算処理を行うためのＣＰＵ（Central Processing Unit）１と、データや

プログラムを記憶する主記憶３（例えば、ＲＡＭ（Random Access Memory）等）、バスブリッジ２と、データやプログラムを記憶する記憶装置５（例えば、ＨＤＤ等）、表示を制御するための表示制御装置６を備える。データ受信装置１０とＣＰＵ１と主記憶３とバスブリッジ２と記憶装置５と表示制御装置６とは相互にＰＣＩ（Peripheral Component Interconnect）バス４で接続されている。尚、記憶装置５は、フロッピー（登録商標）ディスク、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ－ＲＡＭ、ＭＯ等のように、書き込み可能又は書き換え可能な記憶媒体であってもよい。記憶装置は、データ、情報を記憶できればよい。

【００１４】なお、情報処理装置は、PC、ワークステーションの他、携帯電話を含む。

【００１５】データ受信装置１０は、放送データを受信するためのチューナ１１と、暗号化されたコンテンツを復号化するコンテンツ復号器１２と、放送データを暗号化されたコンテンツと暗号化されたスクランブル鍵Ｋｓとに分離する分離器１３と、コンテンツをデコードするコンテンツデコーダ１４と、演算処理を行うためのローカルＣＰＵ１５と、ワーク鍵Ｋｗ及び契約情報を記憶すると共にワーク鍵Ｋｗによって暗号化されたスクランブル鍵Ｋｓを復号化するＩＣカード１６と、再暗号化されたスクランブル鍵Ｋｓを復号化する復号器１７と、再暗号化されたスクランブル鍵Ｋｓを復号化するための鍵とコンテンツＩＤとを記憶する鍵格納領域と、スクランブル鍵Ｋｓを再暗号化するＫｓ暗号器１９と、識別ＩＤを格納する識別ＩＤ格納領域２０と、乱数を発生する乱数発生器２１と、再暗号化されたスクランブル鍵Ｋｓを暗号化されたコンテンツに多重化するＫｓ多重器２２と、ＰＣＩバス４とインターフェースするためのバスＩ／Ｆ部２３とを備える。これら各機器は、ローカルバス２４によって、相互に接続される。尚、チューナ１１は、モデムやＴＡ等のようにネットワークを介して伝送されたデータを受信する受信機であってもよい。また、ＩＣカード１６は、データ受信装置１０から分離（着脱）可能である。ワーク鍵Ｋｗは、ＩＣカード１６に記憶されるのが好ましいが、他の記録媒体（例えば、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等）に記憶されてもよいし、ネットワークによってアクセス可能なサーバに記憶されてもよい。ワーク鍵Ｋｗがサーバに記憶される場合は、ネットワークを介して、ワーク鍵Ｋｗを取得する。

【００１６】次に、情報処理装置の処理内容を説明する。まず、ワーク鍵Ｋｗと契約情報は予めＩＣカード１６に保存されているとする。最初にコンテンツを記録する場合を説明する。チューナ１１により暗号化された放送データ（番組）を受信し、コンテンツ復号器１２を通り分離器１３で、受信された放送データを暗号化されたコンテンツと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵Ｋｓはローカルで、ＣＰＵ１５によりＩＣカード１６でワーク鍵Ｋｗによって復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵ＫｓをＫｓ暗号器１９に転送する。Ｋｓ暗号器１９では、識別ＩＤ格納領域に格納されかつデータ受信装置１０毎のユニークな識別情報である識別ＩＤと乱数発生器２１で生成された乱数をもちいて暗号化する。ＣＰＵ１で指定した再暗号化した事を示すコンテンツＩＤを、バスブリッジ２とバスＩ／Ｆ部２３を介してＫｓ暗号器１９に転送しておく。再暗号化が行われるとＫｓ暗号器１９はコンテンツＩＤと再暗号化したスクランブル鍵ＫｓをＫｓ多重器２２に転送する。また、Ｋｓ暗号器１９は再暗号化されたスクランブル鍵Ｋｓを復号する時に用いる鍵とコンテンツＩＤとを対にして鍵格納領域１８に格納する。Ｋｓ多重器２２ではコンテンツＩＤと再暗号化したスクランブル鍵Ｋｓとを多重化し、バスＩ／Ｆ部２３に転送する。バスＩ／Ｆ部では、この多重化されたデータをＰＣＩバス４、バスブリッジ２を介して主記憶３に転送し、主記憶３にある程度データが貯まったら、ＣＰＵ１でＨＤＤ等の記憶装置５に格納する。

【００１７】記録したコンテンツを再生する場合を説明する。記憶装置５に格納された多重化されたデータをＣＰＵ１で読み出しＰＣＩバス４を介してバスＩ／Ｆ部２３を通してコンテンツ復号器１２に入力する。多重化されたデータは、分離器１３で暗号化されたスクランブル鍵Ｋｓを分離しローカルＣＰＵ１５に送る。ローカルＣＰＵ１５では、再暗号化した事をしめすコンテンツＩＤを確認するとコンテンツＩＤと暗号化されたスクランブル鍵ＫｓをＫｓ復号器１７に転送する。Ｋｓ復号器１７はコンテンツＩＤを元に対応した再暗号化されたスクランブル鍵Ｋｓを復号するための鍵を鍵格納領域１８より読み出し、再暗号化されたスクランブル鍵Ｋｓをこの鍵と識別ＩＤを用いて復号化する。ローカルＣＰＵ１５はこのスクランブル鍵Ｋｓを受け取りコンテンツ復号器１２に設定して、暗号化されたコンテンツを復号化する。この復号されたコンテンツは、コンテンツデコーダ１４によりデコードされた後、出力装置３０に送られ視聴する事ができる。

【００１８】このようにコンテンツを暗号化したままで、スクランブル鍵Ｋｓをデータ受信装置固有の識別ＩＤを用いて再暗号化しコンテンツと多重化して記録することで、例えファイルがコピーされても他の情報処理装置やデータ再生装置で再生しようとしても、識別ＩＤが異なるためスクランブル鍵Ｋｓを復号することができないため、コンテンツの著作権の保護が可能となる。また、鍵格納領域１８に格納される鍵は更新される事がないので再生する場合の時間による制限もなくなる。次に、本発明の特徴であるＫｓ暗号器１９について図４を用いて詳細に説明する。図４において、４１はスクランブル鍵Ｋｓを格納するスクランブル鍵Ｋｓレジスタで、

４２はコンテンツのＩＤを格納するコンテンツＩＤレジスタで、４５はスクランブル鍵Ｋｓを再暗号化するスクランブル鍵暗号部で、４６は暗号化されたスクランブル鍵を復号するための鍵を生成する復号鍵生成部で、４７はスクランブル鍵Ｋｓを暗号化する鍵を生成する暗号鍵生成部で、４８はコンテンツＩＤと再暗号化されたスクランブル鍵Ｋｓを合成する合成部である。Ｋｓ暗号器１９は、スクランブル鍵Ｋｓレジスタ４１と、コンテンツＩＤレジスタ４２と、格納制御部４３と、スクランブル鍵暗号部４５と、復号鍵生成部４６と、暗号鍵生成部４７と、合成部４８とを備える。

【００１９】次に、これらを用いて処理内容を説明する。スクランブル鍵レジスタ４１には、ＩＣカードで復号化されたスクランブル鍵ＫｓがローカルＣＰＵ１５により設定され、コンテンツＩＤレジスタ４２にはＣＰＵ１によってコンテンツＩＤが設定される。暗号鍵生成部４７では、識別ＩＤと乱数発生器２１で生成した乱数に所定の演算を施し暗号化するための鍵を得る。この暗号化するための鍵はスクランブル鍵暗号部４５に送られ、スクランブル鍵レジスタ４１に格納されているスクランブル鍵Ｋｓを暗号化して合成部４８に送られる。合成部４８では、暗号化されたスクランブル鍵Ｋｓとコンテンツ ＩＤレジスタ４２に格納されたコンテンツＩＤを合成して、Ｋｓ多重器２２に送る。ここで、コンテンツＩＤは、暗号化されていないためＣＰＵ１で確認できる事になる。これにより、再生を行う場合、記録されている多重化されたデータのコンテンツＩＤが確認できる。また、復号器生成部４６では、識別ＩＤと乱数発生器２１で生成した乱数に所定の演算を施し復号化するための鍵を得る。格納制御部４３では、この復号化するための鍵とコンテンツＩＤを対にして鍵格納領域１８に格納する。

【００２０】尚、本発明は、放送電波を介して伝送された放送データを受信する場合に限られず、ネットワーク（インターネット、ローカルエリアネットワーク等）を介して伝送されたデータを受信する場合や、他の情報処理装置から伝送されたデータを受信する場合にも適用可能である。

【００２１】次に、図５を用いて第２の実施例を説明する。図５において、３１はコンテンツを再生する時に用いる再生用分離器で、３２はコンテンツを記録するときに用いる記録用分離器である。第１の実施例では、コンテンツを記録している時には暗号化されたままコンテンツを転送するため暗号化されたコンテンツの復号化は行わなかった。つまりコンテンツ復号器１２は動作せずに分離器１３に転送されてくるデータは、暗号化されたままのコンテンツであり当然コンテンツデコーダ１４で復号させることはできない。つまり、記録中はコンテンツを視聴する事ができない。そこで図５の用に再生用分離器３１と記録用分離器３２を独立に持つ事により記録中のコンテンツの視聴を可能としている。

【００２２】処理内容としては次の通りである。再生用分離器３１では、暗号化されたスクランブル鍵Ｋｓを分離してローカルＣＰＵ１５によりＩＣカードでスクランブル鍵Ｋｓを復号しコンテンツ復号器１２に設定して暗号化されたコンテンツの復号を行う。従って、再生用分離器３１から送られてくるコンテンツは復号されているためコンテンツデコーダ１４でデコードでき視聴が可能になる。また、記録用分離器では、復号されているコンテンツは必要ないため、チューナの出力よりデータを受け取り暗号化されたコンテンツを分離してＫｓ多重器２２に転送する事により記憶装置５への記録が可能となる。

【００２３】次に、図６を用いて第３の実施例を説明する。図６において、５２は第１、第２の実施例におけるＫｓ復号器１７、Ｋｓ暗号器１９、識別ＩＤ格納領域２０、乱数発生器２１と鍵格納領域１８の機能を持つ取り外し可能なスクランブル鍵暗号復号カードである。スクランブル鍵暗号復号カード５２は、カードＩ／Ｆ部５１を介してローカルバス２４に接続されており、再暗号化されたスクランブル鍵ＫｓとコンテンツＩＤもカードＩ／Ｆ部５１を介してＫｓ多重器２２に接続されているので、Ｋｓ復号器１７とＫｓ暗号器１８のアクセスは第１、第２の実施例と同様に行える。スクランブル鍵暗号復号カード５２は、データ受信装置１０から分離（着脱）可能である。また、識別ＩＤは、スクランブル鍵暗号復号カード５１毎にユニークなＩＤにするのが好ましい。これにより、例えば記憶装置５に記録された多重化されたデータを、ＤＶＤ－ＲＡＭ、ＣＤ－Ｒ、ＣＤ－ＲＷの様な外部記憶装置８にコピーしてこの外部記憶装置８とスクランブル鍵暗号復号カード５１を本発明のデータ受信装置１０が接続されている情報処理装置であれば他の情報処理装置でもコンテンツの視聴が可能になる。また、スクランブル鍵暗号復号カード５１の機能をＩＣカード１６に内蔵する事でカードの枚数を減らす事も容易に考えられる。

【００２４】次に、図７を用いて第４の実施例を説明する。図７において、３４はコンテンツを再暗号化するコンテンツ暗号器で、３５は再暗号化されたコンテンツを復号する再暗号コンテンツ復号器である。

【００２５】まず、コンテンツを記録する場合を説明する。チューナ１１により暗号化された放送データ（番組）を受信し、コンテンツ復号器１２を通り分離器１３で、暗号化されたコンテンツと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵ＫｓはローカルＣＰＵ１５によりＩＣカード１６で復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵Ｋｓをコンテンツ復号器１２に設定する。コンテンツ復号器１２で復号されたコンテンツは分離器１３によりコンテンツデコーダ１４とコンテンツ暗号器３

４に送られる。コンテンツデコーダ１４でコンテンツをデコードして出力装置３０に出力してコンテンツを視聴できる。コンテンツ暗号器３４では、データ受信装置毎のユニークな識別情報である識別ＩＤと乱数発生器２１で生成された乱数をもちいて暗号化する。

【００２６】また、ＣＰＵ１で指定した再暗号化した事を示すコンテンツＩＤを、バスブリッジ２とバスＩ／Ｆ部２３を介してコンテンツ暗号器３４に転送しておく。再暗号化が行われるとコンテンツ暗号器３４はコンテンツＩＤと再暗号化したコンテンツをバスＩ／Ｆ部２３に転送する。また、コンテンツ暗号器３４は再暗号化されたコンテンツを復号する時に用いる鍵とコンテンツＩＤを鍵格納領域１８に格納する。バスＩ／Ｆ部では、この多重化されたデータをＰＣＩバス４、バスブリッジ２を介して主記憶３に転送し、主記憶３にある程度データが貯まったら、ＣＰＵ１でＨＤＤ等の記憶装置５に格納する。記録したコンテンツを再生する場合を説明する。記憶装置５に格納された再暗号化されたデータをＣＰＵ１で読み出しＰＣＩバス４を介してバスＩ／Ｆ部２３を通して再暗号コンテンツ復号器３５に入力する。この時コンテンツＩＤに対応した鍵を鍵格納領域１８から読み出し再暗号化されたコンテンツを復号して分離器１３に入力してコンテンツＩＤ等の余分なデータを削除してコンテンツデコーダ１４に転送する。コンテンツデコーダ１４によりデコードされ出力装置３０に送られ視聴する事ができる。また、コンテンツ暗号器３４で用いる暗号アルゴリズムを放送事業者がコンテンツを暗号化するときのアルゴリズムと同じにする事によりコンテンツ復号器１２と再暗号コンテンツ復号器３５を共通化する事も可能である。このように、この実施例でも記憶装置５に格納されるコンテンツは、暗号化されているため第１の実施例と同様の効果がある。

【００２７】以上説明したように、本発明の第１～第４の実施例によれば、放送データを受信する装置において暗号化されたコンテンツを復号する暗号化された鍵を復号し再暗号化することで、記憶装置に暗号化されたままのコンテンツを格納でき、ファイル操作を行うことができるアプリケーションが動作するＰＣなどの情報処理装置に於いても、コンテンツの著作権の保護が可能でワーク鍵ｋｗが変更になってもコンテンツを視聴可能なデータ受信装置を提供できる。また、暗号化されたコンテンツを復号する暗号化された鍵を復号し再暗号化する機能を取り外しか可能な構造にする事により、別のデータ処理装置でもコンテンツの視聴が可能になる。

【００２８】尚、上記第１～第４の実施例は、相互に組み合わせることが可能である。上記第１～第４の実施例の各機器の処理は、ハードウェアで実行されてもよりし、プログラム（ソフトウェア）で実行されてもよい。そして、プログラムは、記憶媒体（例えば、フロッピーディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＭＯ等）に記憶されてもよいし、ネットワークを介してアクセス可能なサーバに記憶されてもよい。プログラムがサーバに記憶された場合は、ネットワークを介して、ダウンロードが可能である。

【００２９】以上の実施の形態によれば、暗号化されたコンテンツが復号化できない状態で移動することができるため、コンテンツの著作者等の権利の保護を図りつつ、視聴者側で適切な記憶媒体や記憶装置でコンテンツを管理できるという効果を奏する。

【００３０】次に図８を用いて第５の実施例を説明する。図８において５３は第４の実施例における鍵格納領域１８と識別ＩＤ２０の機能を持つ取り外し可能な鍵格納カードである。鍵格納カード５３は、カードＩ／Ｆ５４を介してコンテンツ暗号器３４と再暗号コンテンツ復号器３５に接続されているので、コンテンツ暗号器３４と再暗号コンテンツ復号器３５のアクセスは第４の実施例と同様に行える。また、第３の実施例で説明したように、識別ＩＤ２０を鍵格納カード５３毎にユニークなＩＤにしておけば、例えば記憶装置５に記録された多重化されたデータを、ＤＶＤ－ＲＡＭの様な外部記憶装置８にコピーしてこの外部記憶装置と鍵格納カード５３を本発明のデジタル放送データ転送処理装置１０が接続されているＰＣであれば他のＰＣでもコンテンツの視聴が可能になることは明らかである。

【００３１】次に図９から１１を用いて第６の実施例を説明する。まず図９を用いて構成を説明する。図９において、６１と６２はそれぞれカードＩ／Ｆ５４を介してデータのやり取りを行う際に暗号通信の制御を行うデジタル放送データ転送処理装置１０側の暗号通信制御部で、鍵格納カード５３側のカード暗号通信制御部である。先述した、第３および５の実施例ではカードＩ／Ｆに鍵の情報がやり取りされ、カードＩ／Ｆのプロトコルがわかっている場合や規格化されていて一般に入手が可能な場合には、ユーザが信号をプローブすることで鍵を知ることが可能である。そこで、カードＩ／Ｆ部５４と鍵格納カード５３の間は暗号通信制御部６１とカード暗号通信制御部を用いてやり取りされるデータを暗号化することで鍵の情報などをユーザが簡単に入手できないようにする。

【００３２】図１０を用いて、鍵を格納する場合の手順について説明する。ここで、Ｋｏは、公開鍵方式の公開鍵でデータを暗号化するときに使用される鍵で、Ｋｐは公開鍵方式の秘密鍵で暗号化されたデータを復号するときに使用される鍵で、Ｋｃは第４の実施例で述べた再暗号化されたコンテンツデータを復号するときに用いるコンテンツ鍵である。暗号通信制御部６１は、自身の認証データと予め保持している秘密鍵Ｋｐと対の公開鍵Ｋｏとを含んだ鍵格納指示を作成し、これを鍵格納カード５３に送信する（Ｔ１００１）。これを受けて鍵格納カード５３のカード暗号通信制御部６２はデジタル放送デー

タ転送処理装置１０の認証を行う（Ｔ１００２）。それからカード暗号通信制御部６２は乱数などを用いてセッション鍵Ｋｓ１を生成し（Ｔ１００３）、これを鍵格納指示に含まれているＫｏを用いて暗号化して、送信元であるデジタル放送データ転送処理装置１０の暗号通信制御部６１に送信する（Ｔ１００４）。これを受けて暗号通信制御部６１は、暗号化されたセッション鍵Ｋｓ１を予め保持している秘密鍵Ｋｐを用いて復号し、セッション鍵Ｋｓ１を得る（Ｔ１００５）。それから乱数Ｋｓ２を生成して（Ｔ１００６）、この乱数Ｋｓ２をセッション鍵Ｋｓ１を用いて暗号化して鍵格納カード５３に送信する（Ｔ１００７）。鍵格納カード５３のカード暗号通信制御部６２では、セッション鍵Ｋｓ１を用いて暗号化された乱数Ｋｓ２を復号し、乱数Ｋｓ２を得る（Ｔ１００８）。そしてコンテンツの暗号化に必要な識別ＩＤ２０を乱数Ｋｓ２を用いて暗号化し暗号通信制御部６１に送信する（Ｔ１００９）。暗号通信制御部６１では、Ｋｓ２を用いて暗号化された識別ＩＤを復号し、識別ＩＤを得て（Ｔ１０１０）、コンテンツ暗号器３４よりコンテンツＩＤとコンテンツを復号するときに必要なライセンス鍵Ｋｃを得て（Ｔ１０１１）、これらをセッション鍵Ｋｓ１を用いて暗号化し鍵格納カード５３に送信する。そして鍵格納カード５３のカード暗号通信制御部６２でＫｓ１を用いて復号化し、コンテンツＩＤとライセンス鍵Ｋｃを得て、これらを鍵格納領域１８に格納する。このように、コンテンツの復号に必要な識別ＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃは、暗号化されてやり取りし、更にこれらの暗号に用いられるセッション鍵Ｋｓ１、乱数Ｋｓ２は、乱数などを用いて生成されるため暗号化されたデータは毎回違うデータとなり、信号をプローブするだけでは鍵を知ることは困難となる。

【００３３】図１１を用いて、コンテンツを復号（再生）する鍵を得る場合の手順について述べる。暗号通信制御部６１は、自身の認証データと予め保持している秘密鍵Ｋｐと対の公開鍵Ｋｏとを含んだ鍵送信指示を作成し、これを鍵格納カード５３に送信する（Ｔ１１０１）。これを受けて鍵格納カード５３のカード暗号通信制御部６２はデジタル放送データ転送処理装置１０の認証を行う（Ｔ１１０２）。それからカード暗号通信制御部６２は乱数などを用いてセッション鍵Ｋｓ１を生成し（Ｔ１１０３）、これを鍵格納指示に含まれているＫｏを用いて暗号化して、送信元であるデジタル放送データ転送処理装置１０の暗号通信制御部６１に送信する（Ｔ１１０４）。これを受けて暗号通信制御部６１は、暗号化されたセッション鍵Ｋｓ１を予め保持している秘密鍵Ｋｐを用いて復号し、セッション鍵Ｋｓ１を得る（Ｔ１１０５）。それから乱数Ｋｓ２を生成して（Ｔ１１０６）、この乱数Ｋｓ２をセッション鍵Ｋｓ１を用いて暗号化して鍵格納カード５３に送信する（Ｔ１１０７）。鍵格納カード５３のカード暗号通信制御部６２では、セッション鍵Ｋｓ１を用いて暗号化された乱数Ｋｓ２を復号し、乱数Ｋｓ２を得る（Ｔ１００８）。そしてコンテンツの復号化に必要な識別ＩＤ２０とライセンス鍵Ｋｃを乱数Ｋｓ２を用いて暗号化し暗号通信制御部６１に送信する（Ｔ１１０９）。暗号通信制御部６１では、Ｋｓ２を用いて暗号化された識別ＩＤとライセンス鍵Ｋｃを復号し、識別ＩＤとライセンス鍵Ｋｃを得て（Ｔ１１１０）、これらの識別ＩＤとライセンス鍵Ｋｃを再暗号コンテンツ復号器３５に送りコンテンツを復号化する。この場合も先述したように、信号をプローブするだけでは鍵を知ることは困難となる。

【００３４】次に図１２を用いて第７の実施例を説明する。図１２において５７は、暗号化したコンテンツデータを格納するコンテンツ格納領域で、５５はコンテンツ格納領域に第６の実施例で説明した暗号通信を用いて識別ＩＤやコンテンツ鍵をやり取りする鍵格納カードの機能を具備した鍵格納領域付記憶装置で、５６は、コンテンツ格納領域５７や鍵格納領域や識別ＩＤをアクセスするためのカード・格納領域Ｉ／Ｆ部である。これらを用いて動作を説明する。最初にコンテンツを記録する場合を説明する。チューナ１１により暗号化された番組を受信し、コンテンツ復号器１２を通り分離器１３で、暗号化されたコンテンツデータと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵ＫｓはローカルＣＰＵ１５によりＩＣカード１６で復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵Ｋｓをコンテンツ復号器１２に設定する。

【００３５】コンテンツ復号器１２で復号されたコンテンツデータは分離器１３によりコンテンツデコーダ１４とコンテンツ暗号器３６に送られる。コンテンツデコーダ１４でコンテンツをデコードして出力装置３０に出力してコンテンツを視聴できる。コンテンツ暗号器３６では、暗号通信を用いて方送受信データ転送処理装置毎のユニークな識別情報である識別ＩＤ２０を取得し、これと乱数発生器２１で生成された乱数をもちいて暗号化する。ここで生成したコンテンツ鍵とコンテンツＩＤを暗号通信を用いて書き格納領域１８に格納する。コンテンツ暗号器３６は再暗号化されたコンテンツデータをカード・格納領域Ｉ／Ｆ部を介してコンテンツＩＤとともにコンテンツ領域５７に格納される。また、復号するときは鍵格納領域付記憶装置５５のコンテンツ格納領域５７に格納された暗号化されたコンテンツデータとコンテンツＩＤを再暗号コンテンツ復号器３７が読み出し、暗号通信を用いてコンテンツＩＤに対応したコンテンツ鍵と識別ＩＤをそれぞれ鍵格納領域１８と識別ＩＤ２０から読み出し、暗号化されたコンテンツデータを復号する。それから、復号化されたコンテンツデータは分離器１３を介してコンテンツデコーダ１４に入力され出力装置３０で出力されコンテンツを視聴することができる。

【００３６】また、鍵格納領域１８はコンテンツを再暗

号化するとその都度コンテンツ鍵が増えていくが、鍵格納領域１８は有限の容量しか持たないため一杯になってしまう場合がある。そのときには鍵格納カードを複数枚で管理することになりユーザが管理するのに不便である。しかし、図１２の様な構成をとれば、コンテンツを格納する領域の容量により、鍵格納領域の容量を適当に決めることにより上記のような問題は少なくなり、またコンテンツと鍵は常に一緒にあるため鍵とコンテンツを分けて管理する必要がなくユーザにとって便利である。コンテンツデータをあるグループ毎にコンテンツ鍵１つに関連付けたり、コンテンツ格納領域をある単位毎に分けそこに格納されるコンテンツ毎に関連図けることにより鍵格納領域の容量を削減することも可能である。また、図１２のコンテンツ格納領域５７は、ＨＤＤや半導体記憶装置であったり、ＤＶＤ－ＲＡＭや磁気テープでもメディアのケースに電極などをつけ鍵格納領域や識別ＩＤを持たせることで鍵格納領域付記憶装置とすること可能である。

【００３７】次に図１３を用いて第８の実施例を説明する。図１３において６９は暗号化コンテンツを復号するときに用いるコンテンツ鍵で、６８はコンテンツ鍵６９に対応した鍵インデックスで、６７は複数のコンテンツ鍵６９と鍵インデックス６８の対を格納する鍵格納領域で、４０は鍵インデックスを暗号化したり復号化したりする鍵インデックス暗号復号器である。

【００３８】これらを用いて動作を説明する。最初にコンテンツを記録する場合を説明する。チューナ１１により暗号化された番組を受信し、コンテンツ復号器１２を通り分離器１３で、暗号化されたコンテンツデータと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵ＫｓはローカルＣＰＵ１５によりＩＣカード１６で復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵Ｋｓをコンテンツ復号器１２に設定する。コンテンツ復号器１２で復号されたコンテンツデータは分離器１３によりコンテンツデコーダ１４とコンテンツ暗号器３８に送られる。コンテンツデコーダ１４でコンテンツをデコードして出力装置３０に出力してコンテンツを視聴できる。コンテンツ暗号器３８では、乱数発生器２１で生成された乱数を用いて鍵格納領域６７の複数あるコンテンツ鍵のどれを使用するかを決める鍵インデックスを生成し、暗号通信を用いてこの鍵インデックスを鍵格納カード６６に送信して、鍵インデックス６８に対応したコンテンツ鍵６９と識別ＩＤ２０を得る。ここで取得したコンテンツ鍵と識別ＩＤを用いてコンテンツデータを暗号化して、更に鍵インデックス暗号復号器４０である特定の鍵を用いて鍵インデックスを暗号化して、暗号化されたコンテンツデータとともにバスＩ／Ｆ部２３を介して主記憶３に転送し最終的には、記憶装置５または外部記憶装置８に格納する。また、鍵インデックス暗号復号器では、ある特定の鍵で暗号化すると暗号化された結果も鍵インデックスが同じであれば同じデータとなってしまうため鍵インデックスに乱数などの冗長なデータをつけて暗号化すれば結果も異なり鍵インデックスが解読される可能性は低くなる。次に記録したコンテンツを再生する場合を説明する。記憶装置５に格納された再暗号化されたデータをＣＰＵ１で読み出しＰＣＩバス４を介してバスＩ／Ｆ部２３を通して再暗号コンテンツ復号器３９に入力する。この時コンテンツデータとともに格納されている暗号化された鍵インデックスを鍵インデックスを鍵インデックス暗号復号器４０で特定の鍵で復号し、鍵インデックスを得る。それから暗号通信を用いて鍵インデックスを鍵格納カードに送信して、鍵インデックス６８に対応したコンテンツ鍵６９と識別ＩＤ２０を得る。そして、再暗号コンテンツ復号器でコンテンツデータを復号して分離器１３に入力してコンテンツＩＤ等の余分なデータを削除してコンテンツデコーダ１４に転送する。コンテンツデコーダ１４によりデコードされ出力装置３０に送られ視聴する事ができる。

【００３９】このような構成にすると、鍵格納カードには新たなコンテンツ鍵を追加する必要がないので暗号化してコンテンツを格納する場合コンテンツの数が増えても、鍵格納カードは増える心配がなく、ユーザも１枚のカード管理すれば良いだけであるので鍵の管理が簡単になり便利である。また、鍵管理カード毎にコンテンツ鍵と識別ＩＤを変えることで暗号化のときに用いた鍵格納カードとは違う鍵格納カードを用いて再生しようとしても同じ鍵インデックスであってもコンテンツ鍵か違いまた識別ＩＤも異なるためコンテンツデータを復号することはできなので、著作権保護が可能となる。

【００４０】以上説明したように、本発明の一実施態様によれば、放送データを受信する装置において暗号化されたコンテンツデータを復号する暗号化された鍵を復号し再暗号化することで、記憶装置に暗号化されたままのコンテンツデータを格納でき、ファイル操作を行うことができるアプリケーションが動作するＰＣなどのデータ処理装置に於いても、コンテンツデータの著作権の保護が可能でワーク鍵ｋｗが変更になってもコンテンツを視聴可能なデジタル放送データ転送処理装置を提供できる。また、暗号化されたコンテンツデータを復号する暗号化された鍵を復号し再暗号化する機能を取り外しか可能な構造にする事により、別のデータ処理装置でもコンテンツの視聴が可能になる。

【００４１】

【発明の効果】本発明の構成により、暗号化されて送信されるコンテンツを保存し、再生することが可能になる。

【図面の簡単な説明】

【図１】本発明の第１の実施例の情報処理装置のシステム構成図である。

17

【図２】従来の限定受信方式のシステム構成図である。

【図３】デジタル放送データを受信し記録する情報処理装置の１システム構成図である。

【図４】本発明の第１の実施例のスクランブル鍵を再暗号化する暗号器のシステム構成図である。

【図５】本発明の第２の実施例の情報処理装置のシステム構成図である。

【図６】本発明の第３の実施例の情報処理装置のシステム構成図。

【図７】本発明の第４の実施例の情報処理装置のシステム構成図。

【図８】本発明の第５の実施例を示すブロック図である。

【図９】暗号通信を用いて鍵を格納するデータのやり取りの一例を示すためのシーケンス図である。

【図１０】暗号通信を用いて鍵を取得するデータのやり取りの一例を示すためのシーケンス図である。

18

【図１１】本発明の第６の実施例を示すブロック図である。

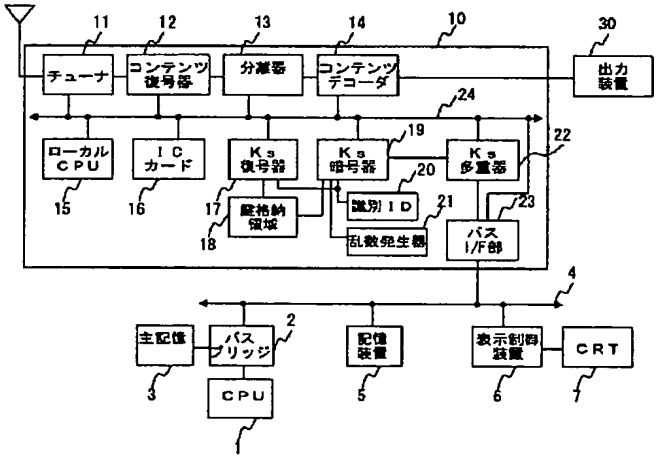
【図１２】本発明の第７の実施例を示すブロック図である。

【図１３】本発明の第８の実施例を示すブロック図である。

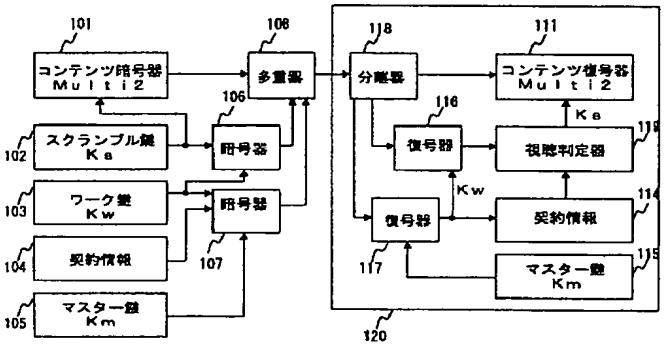
【符号の説明】

１･･･ＣＰＵ、２･･･バスブリッジ、３･･･主記憶、４･･･ＰＣＩバス、５･･･記憶装置、６･･･表示制御部、７･･･ＣＲＴ、８･･･外部記憶装置、１０･･･デジタル放送データ転送処理装置、１１･･･チューナ、１２･･･コンテンツ復号器、１３･･･分離器、１４･･･コンテンツデコーダ、１５･･･ローカルＣＰＵ、１６･･･ＩＣカード、１７･･･Ｋｓ復号器、１８･･･鍵格納領域、１９･･･Ｋｓ暗号器、２０･･･識別ＩＤ、２１･･･乱数発生、２２･･･Ｋｓ多重器、２３･･･バスＩ／Ｆ部、２４･･･ローカルバス、３０･･･出力装置

【図１】

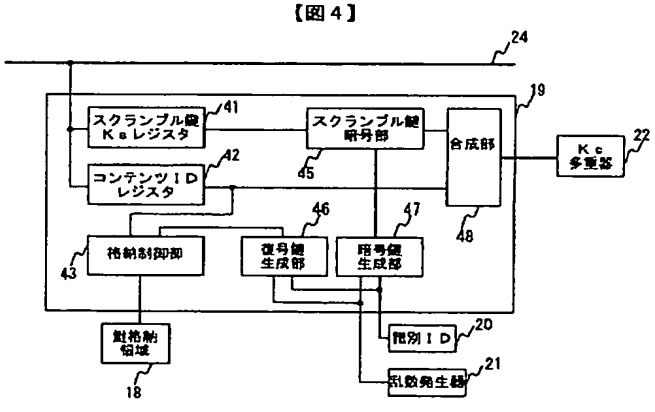


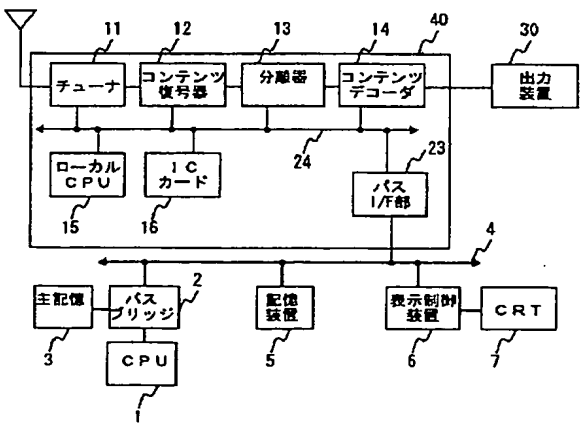
【図２】



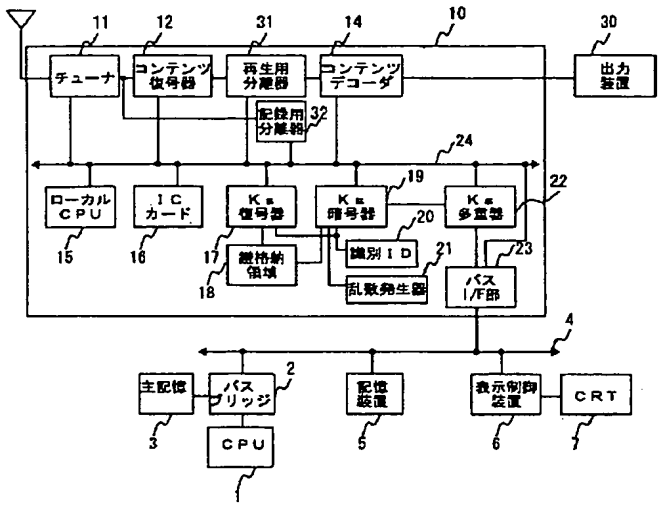
【図３】

【図４】

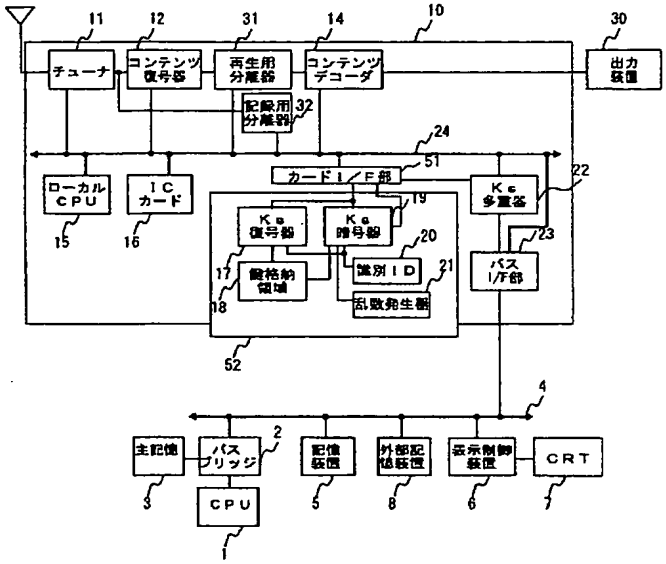




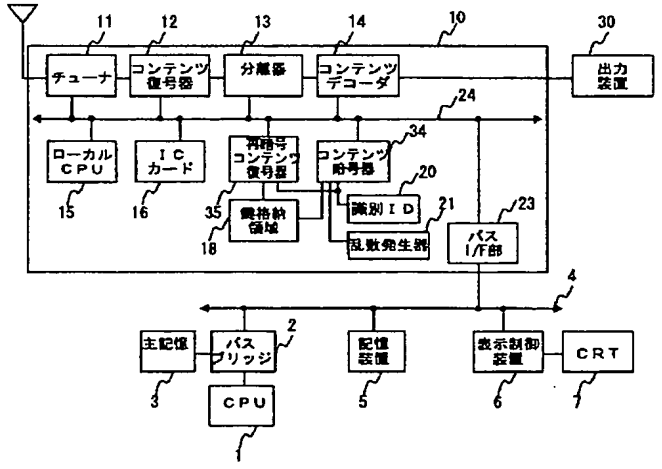
【図５】


チューナ
コンテンツ復号器
再生用分離器
コンテンツデコーダ
出力装置
記録用分離器
ローカルCPU
ICカード
Ks復号器
Ks暗号器
Ks多重器
識別ID
鍵格納領域
乱数発生器
バスI/F部
主記憶
バスブリッジ
CPU
記憶装置
表示制御装置
CRT

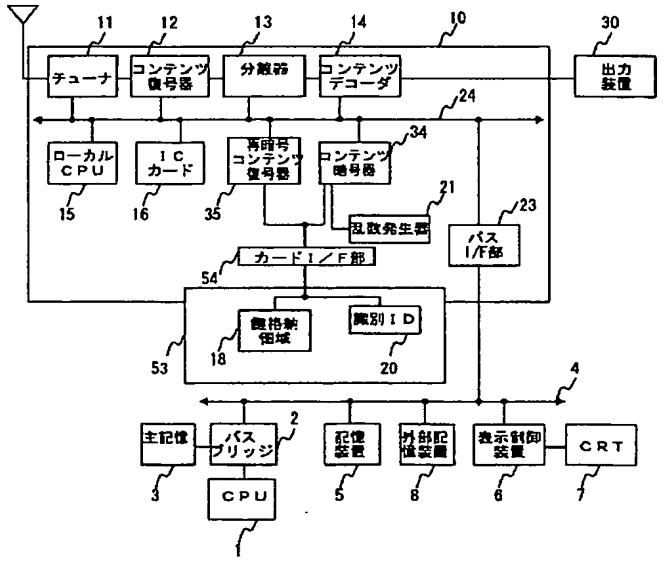
【図６】


チューナ
コンテンツ復号器
再生用分離器
コンテンツデコーダ
出力装置
記録用分離器
カードI／F部
ローカルCPU
ICカード
Ks復号器
Ks暗号器
Ks多重器
識別ID
鍵格納領域
乱数発生器
バスI/F部
主記憶
バスブリッジ
CPU
記憶装置
外部記憶装置
表示制御装置
CRT

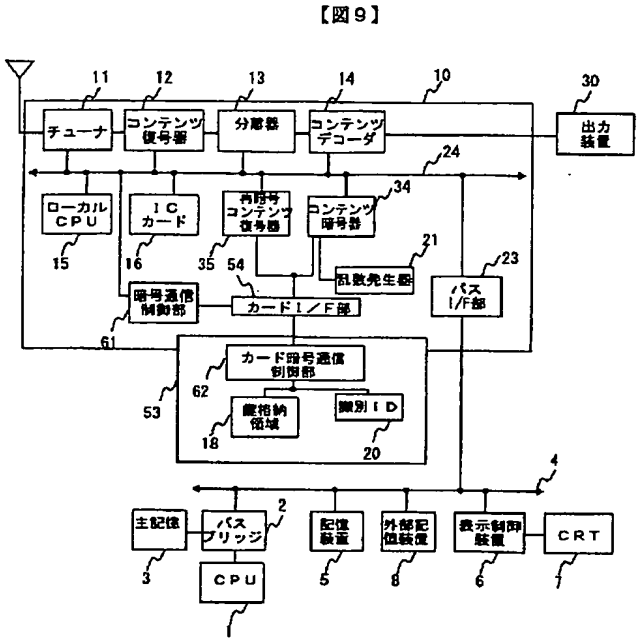
【図７】


チューナ
コンテンツ復号器
分離器
コンテンツデコーダ
出力装置
ローカルCPU
ICカード
再暗号コンテンツ復号器
コンテンツ暗号器
識別ID
鍵格納領域
乱数発生器
バスI/F部
主記憶
バスブリッジ
CPU
記憶装置
表示制御装置
CRT

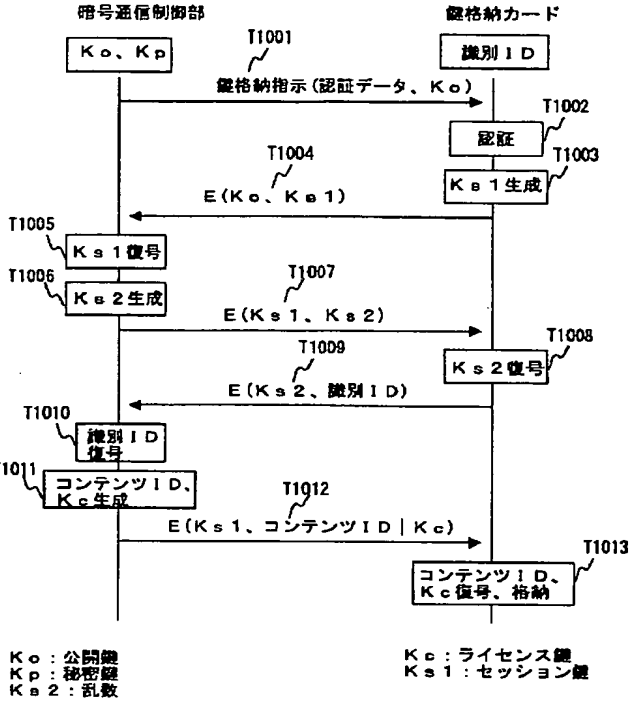
【図８】


チューナ
コンテンツ復号器
分離器
コンテンツデコーダ
出力装置
ローカルCPU
ICカード
再暗号コンテンツ復号器
コンテンツ暗号器
乱数発生器
バスI/F部
カードI／F部
鍵格納領域
識別ID
主記憶
バスブリッジ
CPU
記憶装置
外部記憶装置
表示制御装置
CRT

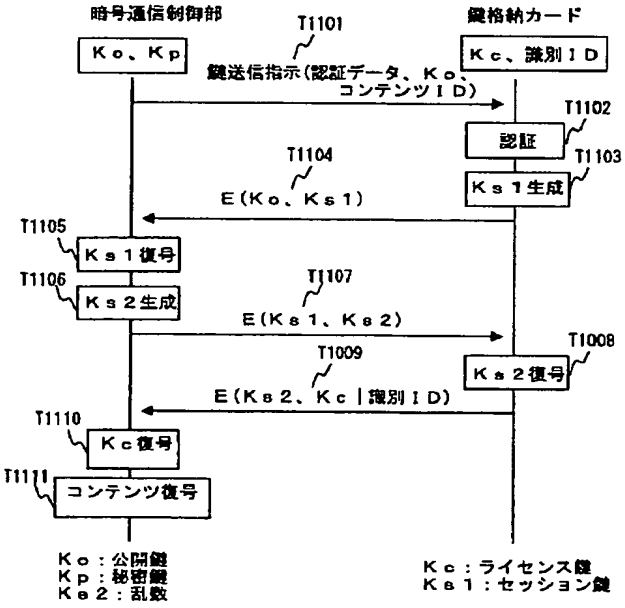
【図９】



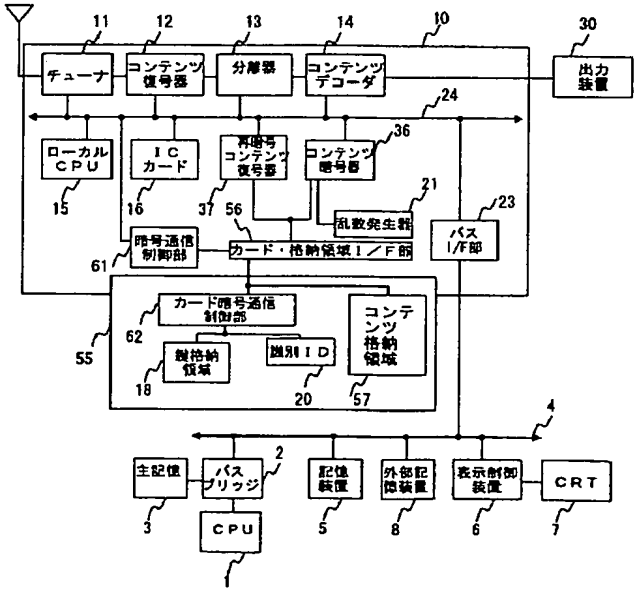
【図１０】



【図１１】

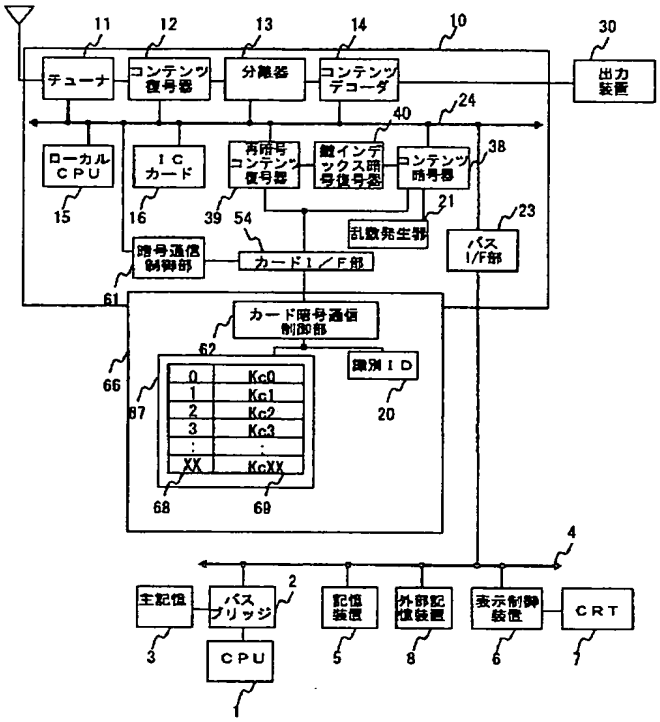


【図１２】



【図１３】

【図１３】



フロントページの続き

(72)発明者　友兼　武郎
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　小楢山　智久
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5J104 AA01 AA16 BA03 EA04 EA26
NA02 PA04 PA05 PA14

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年6月23日(2005.6.23)

【公開番号】特開2002-305512(P2002-305512A)
【公開日】平成14年10月18日(2002.10.18)
【出願番号】特願2001-91685(P2001-91685)
【国際特許分類第７版】
　Ｈ０４Ｌ　9/08
　Ｈ０４Ｈ　1/00
【ＦＩ】
　Ｈ０４Ｌ　9/00　６０１Ａ
　Ｈ０４Ｈ　1/00　Ｆ
　Ｈ０４Ｌ　9/00　６０１Ｄ

【手続補正書】
【提出日】平成16年9月29日(2004.9.29)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
暗号化されたデータであって、前記データが時間の経過により内容が変更されるデータ復号鍵により復号化されるデータを受信するデータ受信装置であって、
第1の暗号鍵により暗号化された前記データを受信する受信器、および
受信された前記データおよび第2の暗号鍵により暗号化された前記データ復号鍵の少なくとも一方を復号化する復号器と接続され、復号化された前記データまたは前記データ復号鍵を、再暗号化鍵により再暗号化する暗号器を有し、
前記暗号器と接続され、再暗号化された前記データおよび再暗号化された前記データ復号鍵のうち少なくとも一方を、記憶媒体に記憶することを特徴とするデータ受信装置。
【請求項２】
請求項１に記載のデータ受信装置であって、
さらに、前記暗号器と接続された多重化器を有し、
前記復号器は、前記データ復号鍵を復号化し、
前記暗号器は、復号化された前記データ復号鍵を暗号化し、
前記多重化器は、再暗号化された前記データ復号鍵と受信された前記データの対応付けを行い、
前記対応付けられた再暗号化された前記データ復号鍵および前記データを、前記記憶媒体に記憶することを特徴とするデータ受信装置。
【請求項３】
請求項２に記載のデータ受信装置であって、
前記暗号器は、当該暗号器で暗号化された前記データ復号鍵を復号する再復号鍵を生成し、再暗号化された前記データ復号鍵と前記復号鍵を互いに関連付けて第２の記憶媒体に記憶することを特徴とするデータ受信装置。
【請求項４】
請求項２に記載のデータ受信装置であって、
さらに、前記受信器に接続された第１の分離器および第２の分離器を有し、
前記受信器は、暗号化された前記データおよび暗号化された前記データ復号鍵を含む送

信情報を受信し、
前記第１の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データを復号化して表示装置に送信し、
前記第2の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データ復号鍵を前記復号器に送信し、分離された前記データを前記多重器に送信することを特徴とするデータ受信装置。
【請求項５】
請求項２に記載のデータ受信装置であって、
前記暗号器は、当該データ受信装置を識別する識別情報に基づいて作成された前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項６】
請求項５に記載のデータ受信装置であって、
前記暗号器は、乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項７】
請求項２に記載のデータ受信装置であって、
前記復号器を有する処理装置と接続するインターフェースユニットを有し、
前記暗号器は、前記処理装置を識別する識別情報に基づいて作成された前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項８】
請求項７に記載のデータ受信装置であって、
前記暗号器は、さらに乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項９】
請求項２に記載のデータ受信装置であって、
当該データ受信装置は、前記記憶媒体をさらに有することを特徴とするデータ受信装置。
【請求項１０】
請求項２に記載のデータ受信装置であって、
当該データ受信装置は、バスを介して前記記憶媒体と接続することを特徴とするデータ受信装置。
【請求項１１】
請求項２に記載のデータ受信装置であって、
さらに、当該データ受信装置の利用者からの入力に応じて、前記暗号器で暗号化された前記データ復号鍵を復号化し、復号化された前記データ復号鍵を用いて前記記憶媒体に記憶された前記データを復号化する第2の復号器、および
前記第2の復号器と接続され、復号化された前記データを出力する出力器を有することを特徴とするデータ受信装置。
【請求項１２】
請求項１に記載のデータ受信装置であって、
前記復号器は、受信された前記データを復号化し、
前記暗号器は、復号化された前記データを暗号化し、暗号化された前記データを復号するための第２の復号鍵を生成し、
前記暗号器で暗号化された前記データを前記記憶媒体に、前記第２の復号鍵を第２の記憶媒体に互いに関連付けて記憶することを特徴とするデータ受信装置。
【請求項１３】
請求項１２に記載のデータ受信装置であって、
さらに、前記受信器に接続された第１の分離器および第２の分離器を有し、
前記受信器は、暗号化された前記データおよび暗号化された前記データ復号鍵を含む送信情報を受信し、

前記第１の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データを復号化して表示装置に送信し、
前記第２の分離器は、前記送信情報を前記データおよび前記データ復号鍵に分離し、分離された前記データを前記復号器に送信することを特徴とするデータ受信装置。
【請求項１４】
請求項１２に記載のデータ受信装置であって、
前記暗号器は、当該データ受信装置を識別する識別情報に基づいて作成された前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項１５】
請求項１４に記載のデータ受信装置であって、
前記暗号器は、さらに乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項１６】
請求項１２に記載のデータ受信装置であって、
さらに、前記復号器を有する処理装置と接続するインターフェースユニットを有し、
前記暗号器は、前記処理装置を識別する識別情報に基づいて作成された前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項１７】
請求項１６に記載のデータ受信装置であって、
前記暗号器は、さらに乱数発生器で発生する乱数に基づいた前記再暗号化鍵を用いることを特徴とするデータ受信装置。
【請求項１８】
請求項１２に記載のデータ受信装置であって、
当該データ受信装置は、前記記憶媒体をさらに有することを特徴とするデータ受信装置。
【請求項１９】
請求項１２に記載のデータ受信装置であって、
当該データ受信装置は、前記記憶媒体とバスを介して接続することを特徴とするデータ受信装置。
【請求項２０】
請求項１２に記載のデータ受信装置であって、
前記第2の記憶媒体を有する第2の処理装置と接続する第2のインターフェースユニットを有することを特徴とするデータ受信装置。
【請求項２１】
請求項１２に記載のデータ受信装置であって、
さらに、当該データ受信装置の利用者からの入力に応じて、前記第2の復号鍵を用いて前記記憶媒体に記憶された前記データを復号化する第2の復号器、および
前記第2の復号器と接続され、復号化された前記データを出力する出力器を有することを特徴とするデータ受信装置。
【請求項２２】
請求項１に記載のデータ受信装置であって、
前記受信器は、放送局から放送される暗号化された前記データおよび所定周期ごとに内容が変更され、暗号化されたデータ復号鍵を含む放送情報を受信することを特徴とするデータ受信装置
【請求項２３】
請求項１に記載のデータ受信装置であって、
前記第1の暗号鍵は、前記第2の暗号鍵であることを特徴とするデータ受信装置。
【請求項２４】
暗号化されたデータであって、前記データが時間の経過により内容が変更されるデータ復号鍵により復号化されるデータを再生するデータ再生装置であって、

記憶媒体から第1の暗号鍵で暗号化された前記データおよび第2の暗号鍵で暗号化された前記データ復号鍵を読み出す手段、
前記データ復号鍵を復号化する手段、
復号された前記データ復号鍵を用いて、読み出されたデータを復号化する手段、および
復号化された前記データを出力する手段とを有することを特徴とするデータ再生装置。
【請求項２５】
請求項３に記載のデータ受信装置であって、さらに、
前記第２の記憶媒体を有する第２の処理装置と接続する第２のインターフェースユニットを有することを特徴とするデータ受信装置。
【請求項２６】
請求項２５に記載のデータ受信装置であって、
前記第２のインターフェースユニットは、暗号通信を用いて、前記第２の記憶媒体に格納される前記再復号鍵を送受信することを特徴とするデータ受信装置。
【請求項２７】
請求項２０に記載のデータ受信装置であって、
前記第２のインターフェースユニットは、暗号通信を用いて、前記第２の記憶媒体に格納される前記再復号鍵を送受信することを特徴とするデータ受信装置。
【請求項２８】
請求項１に記載のデータ受信装置であって、
さらに、前記暗号器と接続され、１以上の鍵を記憶する鍵記憶媒体を有し、
前記暗号器は、前記鍵記憶媒体に記憶された鍵のうち少なくとも１つを用いて、復号化された前記データおよび復号化された前記データ復号鍵のうち少なくとも一方を再暗号化し、前記再暗号化に用いられた鍵と前記再暗号化された前記データおよび再暗号化された前記データ復号鍵のうち少なくとも一方を関連付け、前記再暗号化された前記データおよび再暗号化された前記データ復号鍵のうち少なくとも一方を、前記記憶媒体に格納することを特徴とするデータ受信装置。
【請求項２９】
請求項１に記載のデータ受信装置であって、
前記暗号器は、少なくとも復号化された前記データを再暗号化することを特徴とするデータ受信装置。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-305512

(43)Date of publication of application : 18.10.2002

(51)Int.Cl. H04L 9/08
H04H 1/00

(21)Application number : 2001-091685

(22)Date of filing : 28.03.2001

(71)Applicant : HITACHI LTD

(72)Inventor : MORINO TOKAI
OKAYAMA YUKO
TOMOKANE TAKEO
KOHIYAMA TOMOHISA

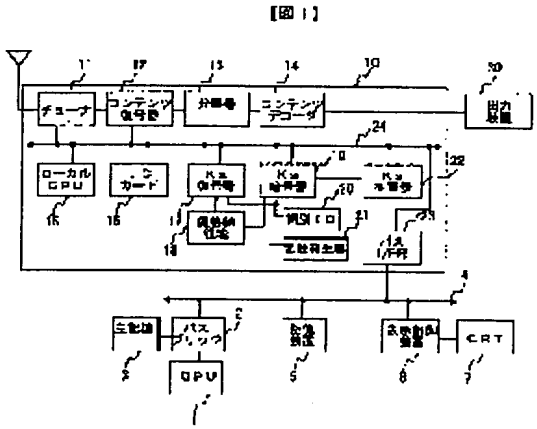
(30)Priority

Priority number : 2001025011 Priority date : 01.02.2001 Priority country : JP

(54) DATA RECEIVING APPARATUS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data receiving apparatus that can protect the copyright of contents and can listen/view contents even if a work key kw is changed even for an information processing apparatus such as a PC on which file utility applications run in a broadcast data receiving apparatus for receiving broadcast data.



SOLUTION: The data receiving apparatus has a tuner 11 for receiving enciphered contents and an enciphered scramble key, a local CPU 15 for deciphering the enciphered scramble key by using a work key in an IC card 16, a Ks encipher unit 17 for generating an encipher key for re-enciphering the deciphered scramble key and a decipher key for re-deciphering the re- enciphered scramble key in accordance with an identification ID specific to the apparatus 10 and an arbitrary random number and for re-enciphering the deciphered scramble key by using the encipher key, a key storage area 18 for storing the decipher key, and a bus I/F unit 23 for

transferring the re- enciphered scramble key and enciphered contents to an external apparatus.

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]In a data receiver which receives data which is the enciphered data and said data decrypts with a data decryption key with which the contents are changed by the passage of time, A receiver which receives said data which has the following composition, and which was enciphered by the 1st encryption key, And it is connected with a decoder which decrypts at least one side of said data decryption key enciphered by said data and the 2nd encryption key which were received, It has a code machine which re-enciphers said decrypted data or said data decryption key with a re-enciphering key, and it is connected with said code machine and at least one side is memorized to a storage among said re-enciphered data and said re-enciphered data decryption key.
[Claim 2]In the data receiver according to claim 1, have further the multiplexing machine connected with said code machine, and said decoder, Decrypt said data decryption key and said code machine, encipher said decrypted data decryption key and said multiplexing machine matches said re-enciphered data decryption key and said received data -- said -- said matched data decryption key which was re-enciphered and said data are memorized to said storage.
[Claim 3]In the data receiver according to claim 2, said code machine generates a re-decode key which decodes said data decryption key enciphered with the code machine concerned, associates said re-enciphered data decryption key and said decode key of each other, and memorizes them to the 2nd storage.
[Claim 4]In the data receiver according to claim 2, have further the 1st eliminator and 2nd eliminator that were connected to said receiver, and said receiver, Receive and transmit information containing said enciphered data and said enciphered data decryption key said 1st eliminator, Divide said transmit information into said data and said data decryption key, decrypt said separated data, transmit to a display and said 2nd eliminator, Said transmit information is divided into said data and said data decryption key, said separated data decryption key is

transmitted to said decoder, and said separated data is transmitted to said multiplex machine.
[Claim 5]In the data receiver according to claim 2, said re-enciphering key created based on identification information which identifies the data receiver concerned is used for said code machine.
[Claim 6]In the data receiver according to claim 5, said re-enciphering key based on a random number by which it is further generated with a random number generator is used for said code machine.
[Claim 7]In the data receiver according to claim 2, it has an interface unit further connected with a processing unit which has said decoder, and said re-enciphering key created based on identification information which identifies said processing unit is used for said code machine.
[Claim 8]In the data receiver according to claim 7, said re-enciphering key based on a random number by which it is further generated with a random number generator is used for said code machine.
[Claim 9]In the data receiver according to claim 2, the data receiver concerned has said storage further.
[Claim 10]In the data receiver according to claim 2, the data receiver concerned is connected with said storage via a bus.
[Claim 11]In the data receiver according to claim 2, further according to an input from a user of the data receiver concerned, It has an output machine which is connected with the 2nd decoder that decrypts said data which decrypted said data decryption key enciphered with said code machine, and was memorized by said storage using said decrypted data decryption key, and said 2nd decoder, and outputs said decrypted data.
[Claim 12]In the data receiver according to claim 1, said decoder, Decrypt said received data and said code machine, The 2nd decode key for enciphering said decrypted data and decoding said enciphered data is generated, to said storage, said 2nd decode key of each other is related with the 2nd storage, and said data enciphered with said code machine is memorized.
[Claim 13]In the data receiver according to claim 12, have further the 1st eliminator and 2nd eliminator that were connected to said receiver, and said receiver, Receive and transmit information containing said enciphered data and said enciphered data decryption key said 1st eliminator, Said transmit information is divided into said data and said data decryption key, said separated data is decrypted, and it transmits to a display, and said 2nd eliminator divides said transmit information into said data and said data decryption key, and transmits said separated data to said decoder.
[Claim 14]In the data receiver according to claim 12, said re-enciphering key created based on identification information which identifies the data receiver concerned is used for said code machine.

[Claim 15]In the data receiver according to claim 14, said re-enciphering key based on a random number by which it is further generated with a random number generator is used for said code machine.
[Claim 16]In the data receiver according to claim 12, it has an interface unit further connected with a processing unit which has said decoder, and said re-enciphering key created based on identification information which identifies said processing unit is used for said code machine.
[Claim 17]In the data receiver according to claim 16, said re-enciphering key based on a random number by which it is further generated with a random number generator is used for said code machine.
[Claim 18]In the data receiver according to claim 12, the data receiver concerned has said storage further.
[Claim 19]In the data receiver according to claim 12, the data receiver concerned is connected with said storage via a bus.
[Claim 20]In the data receiver according to claim 12, it has the 2nd interface unit linked to the 2nd processing unit that has said 2nd storage.
[Claim 21]In the data receiver according to claim 12, further according to an input from a user of the data receiver concerned, It has an output machine which is connected with the 2nd decoder that decrypts said data memorized by said storage using said 2nd decode key, and said 2nd decoder, and outputs said decrypted data.
[Claim 22]In the data receiver according to claim 1, said receiver receives broadcast information which the contents are changed for every said enciphered data which is broadcast from a broadcasting station, and given period, and contains an enciphered data decryption key,
[Claim 23]In the data receiver according to claim 1, said 1st encryption key is said 2nd encryption key.
[Claim 24]In a data reproduction apparatus with which it is the enciphered data and said data reproduces data decrypted with a data decryption key with which the contents are changed by the passage of time,A means which reads said data decryption key enciphered with said data enciphered with the 1st encryption key, and the 2nd encryption key from a storage which has the following composition, A means to decrypt read data using a means to decrypt said data decryption key, and said decoded data decryption key, and a means to output said decrypted data.
[Claim 25]In the data receiver according to claim 3, it has the 2nd interface unit further connected with the 2nd processing unit that has said 2nd storage.
[Claim 26]In the data receiver according to claim 25, said 2nd interface unit transmits and receives said re-decode key stored in said 2nd storage using encryption communication.
[Claim 27]In the data receiver according to claim 20, said 2nd interface unit transmits and receives said re-decode key stored in said 2nd storage using encryption communication.

[Claim 28]In the data receiver according to claim 1, it is connected with said code machine, have further, a key storage which memorizes one or more keys, and said code machine, At least one side is re-enciphered among said decrypted data and said decrypted data decryption key using at least one of keys memorized by said key storage, At least one side is associated among a key used for said re-encryption, said said re-enciphered data, and said re-enciphered data decryption key, and at least one side is stored in said storage among said said re-enciphered data and said re-enciphered data decryption key.
[Claim 29]In the data receiver according to claim 1, said code machine re-enciphers said data decrypted at least.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the information processor which has a data receiver which receives the enciphered contents, and its data receiver. It is related with the information processor which has a data receiver which receives digital broadcasting data and the data transmitted via the network also especially in it, and its data receiver. A television set (tuner), a VCR, a set top box, etc. are contained in a data receiver. A personal computer, a workstation, and a cellular phone are contained in an information processor.
[0002]
[Description of the Prior Art]In recent years, data distribution which provides a user with the enciphered image or sound content by electronic distribution using satellite broadcasting etc. is performed. "BS-digital-broadcasting restricted reception system" The method of the limited reception in BS digital broadcasting is described by ARIB-STD-B25. The restricted reception system which receives the enciphered data in BS digital broadcasting which is this descriptive content is shown in drawing 2.
[0003]Data flow is explained using this drawing 2. First, contents, such as an image and a sound, are enciphered using scramble key Ks102 with the contents code machine 101. Scramble key Ks102 is enciphered using the work key 103 with the code machine 106, and work key Kw103 and the contract information 104 are enciphered using master key Km105 with the code machine 107. These enciphered contents, the scramble key Ks and the work key Ks, and contract information are multiplexed with the multiplex machine 108, and are distributed to a receiver. It separates into the contents, the scramble key Ks and the work key Kw which were enciphered using the eliminator 118, and contract information in the receiver 120. The work key Kw and contract information which were enciphered are decoded using the master key 115 with the decoder 117, and acquire and save the work key Kw and the contract

information 114. The enciphered scramble key is decoded using the work key Kw with the decoder 116, and obtains the scramble key Ks. It judges whether it can view and listen to the enciphered contents by the viewing-and-listening judging device 119 using the contract information 119, and if possible, it will be decrypted using the scramble key Ks with the contents decoder 111. Although it is enciphered and is received by all the receivers, the scramble key Ks is data for every receiver, and it is enciphered with the unique master key Km for every receiver, and it cannot decrypt the work key Kw and contract information here except other receivers. Since Kw required in order to decrypt the scramble key Ks is not obtained, the contents a contract of is not made [whether it carried out and] can be received. Although the master key Km is not changed, the work key Kw will be changed from the time of a contract, and a year half [about] in about one year, and the scramble key Ks will be updated per about several seconds. For this reason, even if the work key Kw of the contents a contract of is not made was found, when the scramble key Ks is found for about one year, viewing and listening only about several seconds is only impossible. The decoder 116 of drawing 2, the decoder 117, the master key 115, the contract information 114, and the viewing-and-listening judging device 119 are realized by the IC card.

[0004]The receiving board of BS digital broadcasting connectable with a personal computer (PC) exists like drawing 3.

[0005]

[Problem(s) to be Solved by the Invention]In recording contents, the following problems arise. Although the case where this problem is shown in drawing 3 is explained to an example, even when a receiving board is in the information processor containing PC, and it is a television set, a set top box, and a VCR, the same problem arises.

[0006]It is as follows when the receiving board of BS digital broadcasting is connected to a personal computer (PC) like drawing 3, and PC realizes a recording machine. The digital data received with the tuner 11 separates scramble key Ks and the work key Kw which were enciphered with the eliminator 13, and contract information, and is sent to IC card 16 by local CPU15 via the local bus 24. In IC card 16, as mentioned above, the work key Kw and contract information are saved and the enciphered SUKURAMPURU key Ks is decrypted. And the scramble key Ks is sent to the contents decoder 12, and the enciphered contents are decrypted. The decrypted contents are decoded by the contents decoder 14, and are outputted to the output units 30, such as a monitor and a loudspeaker. At this time, carrying out a direct output to the display control 6 of PC instead of the output unit 30 is also considered. In order to record on the memory storage 5 like HDD of PC, the contents separated with the eliminator 13 are sent to the bus I/F part 23 from the local bus 24, and it is stored in the main memory 3 via the bus bridge 2 via PCI bus 4 which is an internal bus of PC. It is stored in the memory storage 5 by CPU1 when contents are accumulated to some extent in the main memory 3.

Here, the contents stored in the memory storage 5 are not enciphered, but if the application which performs a file operation is used, a copy will be made simply and protection of the copyright of contents will become difficult.

[0007]In order to protect the copyright of contents, while contents and the scramble key Ks had been enciphered, when it stores in the memory storage 5 and reproduces, it is possible to decode a code, but this, Since the work key Kw will be changed in about one year after half a year as mentioned above, after recording, when time passes, there is a problem said that it will become impossible to view and listen to contents.

[0008]

[Means for Solving the Problem]The purpose of this invention is to provide a data receiver and an information processor which can manage contents with a suitable storage or memory storage by the televiewer side, aiming at protection of rights, such as an author of contents.

[0009]This invention is the enciphered data in order to attain this purpose, It is considered as a data object which said data decrypts with a data decryption key with which the contents are changed by the passage of time, At least one side of said data decryption key which received said data enciphered by the 1st encryption key, and was enciphered by said data and the 2nd encryption key which were received is decrypted, Said decrypted data or said data decryption key is enciphered with a re-enciphering key, it is connected with said code machine and said enciphered data or said data decryption key is memorized to a storage.

[0010]Reproducing data memorized by storage is also included in this invention.

[0011]

[Embodiment of the Invention]Next, the example of this invention is described in detail using a drawing. Drawing 1 is a block diagram showing one information processor of this invention. It is Ks code machine with which 19 re-enciphers a scramble key in drawing 1, 20 is a discernment ID storing region which stores discernment ID (Identifier) which is every data receiver 10 or the unique identification information for every information processor, 21 is a random number generator made to generate a random number, and 18 is a key storing region which stores the key which decrypts the scramble key enciphered with ID and Ks code machine 19 of contents. 22 is a Ks multiplex machine which multiplexes to the contents which are having the re-enciphered scramble key Ks enciphered. 17 is a decoder which decodes the re-enciphered scramble key Ks.

[0012]An information processor is provided with the following.

The data receiver 10 which receives data and performs decryption and re-encryption.

The output unit 30 for viewing and listening to data.

The information processor body which performs information processing.

CRT(Cathode-Ray Tube) 7 for displaying.

CRT7 may be other displays which display the data of a liquid crystal display, a plasma

display, an EL display, etc.
[0013]CPU(Central Processing Unit) 1 for an information processor body to perform data processing, It has the display control 6 for controlling the memory storage 5 (for example, HDD etc.) and the display which remember data and a program to be the main memory 3 which memorizes data and a program, and the bus bridges (for example, RAM (Random Access Memory) etc.) 2. The data receiver 10, CPU1, the main memory 3, the bus bridge 2, the memory storage 5, and the display control 6 are mutually connected by PCI (Peripheral Component Interconnect) bus 4. The memory storage 5 may be a storage possible [writing] or rewritable like a floppy (registered trademark) disk, CD-R, CD-RW, DVD-R, DVD-RW, DVD-RAM, and MO. The memory storage just memorizes data and information.
[0014]An information processor contains a cellular phone besides PC and a workstation.
[0015]The tuner 11 for the data receiver 10 to receive broadcast data, The eliminator 13 divided into the contents decoder 12 which decrypts the enciphered contents, and the scramble key Ks enciphered as the contents which had broadcast data enciphered, The contents decoder 14 which decodes contents, and local CPU15 for performing data processing, IC card 16 which the work key Kw and contract information are memorized, and decrypts the scramble key Ks enciphered by the work key Kw, The key storing region which memorizes the decoder 17 which decrypts the re-enciphered scramble key Ks, and the key and content ID for decrypting the re-enciphered SUKURAMPURU key Ks, Ks code machine 19 which re-enciphers the scramble key Ks, and the discernment ID storing region 20 which stores discernment ID, It has the random number generator 21 which generates a random number, the Ks multiplex machine 22 multiplexed to the contents which had the re-enciphered scramble key Ks enciphered, and the bus I/F part 23 for interfacing with PCI bus 4. These each apparatus is mutually connected by the local bus 24. The tuner 11 may be a receiver which receives the data transmitted via the network like the modem or TA. IC card 16 is separable from the data receiver 10 (attachment and detachment). Although it is preferred that IC card 16 memorizes as for the work key Kw, it may be memorized by other recording media (for example, CD-ROM, DVD-ROM, etc.), and may be memorized by the accessible server with a network. When the work key Kw is memorized by the server, the work key Kw is acquired via a network.
[0016]Next, the contents of processing of an information processor are explained. First, the work key Kw and contract information assume that it is saved beforehand at IC card 16. The case where contents are recorded first is explained. It separates into the scramble key Ks enciphered as the contents which had the broadcast data which received the broadcast data (program) enciphered by the tuner 11, and was received with the eliminator 13 through the contents decoder 12 enciphered. The separated scramble key Ks which was enciphered transmits the scramble key Ks which was decrypted by local CPU15 with the work key Kw by

IC card 16, and was decrypted by local CPU15 to Ks code machine 19. In Ks code machine 19, with the random number which was stored in the discernment ID storing region, and was generated with discernment ID which is the unique identification information for every data receiver 10, and the random number generator 21, are and it enciphers. The content ID which shows the re-enciphered thing which specified by CPU1 is transmitted to Ks code machine 19 via the bus bridge 2 and the bus I/F part 23. The scramble key Ks which re-enciphered Ks code machine 19 as content ID as re-encryption is performed is transmitted to the Ks multiplex machine 22. Ks code machine 19 makes a pair the key and content ID which are used when decoding the re-enciphered SUKURAMPURU key Ks, and stores them in the key storing region 18. With the Ks multiplex machine 22, the scramble key Ks re-enciphered as content ID is multiplexed, and it transmits to the bus I/F part 23. In a bus I/F part, if this multiplexed data is transmitted to the main memory 3 via PCI bus 4 and the bus bridge 2 and data accumulates in the main memory 3 to some extent, it stores in the memory storage 5, such as HDD, by CPU1.

[0017]The case where the recorded contents are reproduced is explained. The multiplexed data which was stored in the memory storage 5 is read by CPU1, and is inputted into the contents decoder 12 through the bus I/F part 23 via PCI bus 4. The multiplexed data separates the scramble key Ks enciphered with the eliminator 13, and sends it to local CPU15. In local CPU15, a check of the content ID which shows having re-enciphered will transmit the scramble key Ks enciphered as content ID to the Ks decoder 17. The Ks decoder 17 reads the key for decoding the re-enciphered scramble key Ks corresponding to origin for content ID from the key storing region 18, and decrypts the re-enciphered scramble key Ks using this key and discernment ID. Local CPU15 receives this scramble key Ks, sets it as the contents decoder 12, and decrypts the enciphered contents. After being decoded by the contents decoder 14, these decoded contents are sent to the output unit 30, and it can view and listen to them.
[0018]By thus, the thing for which it re-enciphers using discernment ID peculiar to a data receiver, and the scramble key Ks is multiplexed with contents, and is recorded with contents enciphered. Since discernment ID differs and the scramble key Ks cannot be decoded even if a metaphor file is copied, and it is going to reproduce with other information processors and data reproduction apparatus, protection of the copyright of contents is attained. The restriction of the key stored in the key storing region 18 by the time in the case of reproducing, since it is not updated is also lost. Next, Ks code machine 19 which is the feature of this invention is explained in detail using drawing 4. It is a scramble key Ks register in which 41 stores the scramble key Ks in drawing 4, 42 is a content ID register which stores ID of contents, and 45 is a scramble key cryptopart which re-enciphers the scramble key Ks, 46 is a decode key generation part which generates the key for decoding the enciphered scramble key, 47 is an encryption key generation part which generates the key which enciphers the scramble key Ks,

and 48 is a synchronizer which compounds the scramble key Ks re-enciphered as content ID. Ks code machine 19 is provided with the following.
Scramble key Ks register 41.
Content ID register 42.
Storing control section 43.
The scramble key cryptopart 45, the decode key generation part 46, the encryption key generation part 47, and the synchronizer 48.

[0019]Next, the contents of processing are explained using these. The scramble key Ks decrypted by the IC card is set to the scramble key register 41 by local CPU15, and content ID is set to the content ID register 42 by CPU1. In the encryption key generation part 47, the key for performing a predetermined operation to the random number generated with discernment ID and the random number generator 21, and enciphering by them is obtained. The key for [this] enciphering is sent to the scramble key cryptopart 45, enciphers the scramble key Ks stored in the scramble key register 41, and is sent to the synchronizer 48. In the synchronizer 48, the enciphered scramble key Ks and the content ID stored in the content ID register 42 are compounded, and it sends to the Ks multiplex machine 22. Here, since it is not enciphered, content ID can be checked by CPU1. Thereby, when reproducing, the content ID of the multiplexed data which is recorded can be checked. In the decoder generation part 46, the key for performing and decrypting a predetermined operation by the random numbers generated with discernment ID and the random number generator 21 is obtained. In the storing control section 43, the key and content ID for [this] decrypting are made into a pair, and it stores in the key storing region 18.
[0020]This invention is not restricted when receiving the broadcast data transmitted via the broadcasting electric-wave, but when receiving the data transmitted via networks (the Internet, a Local Area Network, etc.), or also when receiving the data transmitted from other information processors, it can be applied.
[0021]Next, the 2nd example is described using drawing 5. In drawing 5, 31 is an eliminator for reproduction used when reproducing contents, and 32 is an eliminator for record used when recording contents. In the 1st example, decryption of the contents enciphered in order to transmit contents, while recording contents and it had been enciphered was not performed. That is, the contents decoders 12 are contents enciphered and, naturally cannot make the data transmitted to the eliminator 13 without operating decode by the contents decoder 14. That is, it cannot view and listen to contents during record. Then, viewing and listening of the contents under record is enabled by having independently the eliminator 31 for reproduction, and the eliminator 32 for record in the business of drawing 5.
[0022]As contents of processing, it is as follows. In the eliminator 31 for reproduction, the

enciphered scramble key Ks is separated, the scramble key Ks is decoded by an IC card by local CPU15, and the contents which set it as the contents decoder 12 and were enciphered are decoded. Therefore, since the contents sent from the eliminator 31 for reproduction are decoded, it can decode by the contents decoder 14 and viewing and listening becomes possible. In the eliminator for record, since the contents decoded are unnecessary, they become recordable to the memory storage 5 by separating the contents which received data and were enciphered from the output of the tuner, and transmitting to the Ks multiplex machine 22.

[0023]Next, the 3rd example is described using drawing 6. In drawing 6, 52 is a dismountable scramble key code decoding card with the function of the Ks decoder 17 in the 1st and 2nd example, Ks code machine 19, the discernment ID storing region 20, and the random number generator 21 and the key storing region 18. The scramble key code decoding card 52 is connected to the local bus 24 via the card I/F part 51, Since the scramble key Ks and content ID which were re-enciphered are also connected to the Ks multiplex machine 22 via the card I/F part 51, access of the Ks decoder 17 and Ks code machine 18 can be performed like the 1st and 2nd example. The scramble key code decoding card 52 is separable from the data receiver 10 (attachment and detachment). As for discernment ID, it is preferred to use unique ID every scramble key code decoding card 51. By this the multiplexed data which was recorded, for example on the memory storage 5, If it is the information processor which is copied to DVD-RAM, CD-R, and the external storage 8 like CD-RW and by which the scramble key code decoding card 51 is connected with this external storage 8 in the data receiver 10 of this invention, viewing and listening of contents will be attained with other information processors. Reducing the number of sheets of a card by building the function of the scramble key code decoding card 51 in IC card 16 is also considered easily.

[0024]Next, the 4th example is described using drawing 7. In drawing 7, 34 is a contents code machine which re-enciphers contents, and 35 is a re-code contents decoder which decodes the re-enciphered contents.

[0025]First, the case where contents are recorded is explained. The broadcast data (program) enciphered by the tuner 11 is received, and it separates into the scramble key Ks enciphered as the contents enciphered with the eliminator 13 through the contents decoder 12. The separated scramble key Ks which was enciphered sets the scramble key Ks which was decrypted by local CPU15 by IC card 16, and was decrypted by local CPU15 as the contents decoder 12. The contents decoded with the contents decoder 12 are sent to the contents decoder 14 and the contents code machine 34 by the eliminator 13. Contents are decoded by the contents decoder 14, and it outputs to the output unit 30, and can view and listen to contents. In the contents code machine 34, with the random number generated with discernment ID which is the unique identification information for every data receiver, and the

random number generator 21, are and it enciphers.
[0026]The content ID which shows the re-enciphered thing which specified by CPU1 is transmitted to the contents code machine 34 via the bus bridge 2 and the bus I/F part 23. The contents which re-enciphered the contents code machine 34 as content ID as re-encryption is performed are transmitted to the bus I/F part 23. The contents code machine 34 stores the key and content ID which are used when decoding the re-enciphered contents in the key storing region 18. In a bus I/F part, if this multiplexed data is transmitted to the main memory 3 via PCI bus 4 and the bus bridge 2 and data accumulates in the main memory 3 to some extent, it stores in the memory storage 5, such as HDD, by CPU1. The case where the recorded contents are reproduced is explained. The re-enciphered data which was stored in the memory storage 5 is read by CPU1, and is inputted into the re-code contents decoder 35 through the bus I/F part 23 via PCI bus 4. The contents which read the key corresponding to content ID from the key storing region 18 at this time, and were re-enciphered are decoded, it inputs into the eliminator 13, the excessive data of content ID etc. is deleted, and it transmits to the contents decoder 14. It is decoded by the contents decoder 14, is sent to the output unit 30, and can view and listen. It is also possible to communalize the contents decoder 12 and the re-code contents decoder 35 by making the same as an algorithm in case a broadcasting organization enciphers contents the cryptographic algorithm used with the contents code machine 34. Thus, since it is enciphered, the contents stored in the memory storage 5 also in this example have the same effect as the 1st example.
[0027]By according to the 1st - the 4th example of this invention, decoding the enciphered key which decodes the contents enciphered in the device which receives broadcast data, and re-enciphering, as explained above. Also in information processors, such as PC in which the application which can store the contents enciphered by memory storage and can perform a file operation operates, Even if protection of the copyright of contents is possible and the work key kw is changed, the data receiver which can view and listen to contents can be provided. With [the function which decodes the enciphered key which decodes the enciphered contents and is re-enciphered] removal or a possible structure, viewing and listening of contents is attained also with another data processing device.
[0028]The above 1st - the 4th example can be combined mutually. Even if the above 1st - processing of each apparatus of the 4th example are performed by hardware, they are carried out more, and they may be performed by a program (software). And a program may be memorized by storages (for example, a floppy disk, CD-ROM, DVD-ROM, MO, etc.), and may be memorized by the accessible server via a network. When a program is memorized by the server, it can download via a network.
[0029]The effect that contents are manageable with a suitable storage and memory storage by the televiewer side is done so, aiming at protection of rights, such as an author of contents,

since it can move in the state where the enciphered contents cannot be decrypted according to an above embodiment.

[0030]Next, the 5th example is described using drawing 8. In drawing 8, 53 is a dismountable key storing card with the function of key storing region [in the 4th example] 18, and discernment ID20. Since it is connected to the contents code machine 34 and the re-code contents decoder 35 via card I/F54, the key storing card 53 can perform access of the contents code machine 34 and the re-code contents decoder 35 like the 4th example. If discernment ID20 is set to unique ID every key storing card 53 as the 3rd example explained, For example, the multiplexed data which was recorded on the memory storage 5, If it is PC which is copied to the external storage 8 like DVD-RAM and by which the key storing card 53 is connected with this external storage in the digital broadcasting data transfer processor 10 of this invention, other PCs of attain [viewing and listening of contents] are clear.

[0031]Next, the 6th example is described using 11 from drawing 9. Composition is first explained using drawing 9. In drawing 9, when 61 and 62 exchange data via card I/F54, respectively, they are the encryption communication control sections by the side of the digital broadcasting data transfer processor 10 which controls encryption communication, and they are the card encryption communication control sections by the side of the key storing card 53. It is possible to get to know a key because the information on a key is exchanged by card I/F in the example of the 3rd and 5 which carried out point **, are standardized when the protocol of card I/F is known, and a user generally does the probe of the signal when it can obtain. Then, a user is prevented from the information on a key, etc. coming to hand simply by enciphering the data which the encryption communication control section 61 and a card encryption communication control section are used between the card I/F part 54 and the key storing card 53, and is carried out.

[0032]The procedure in the case of storing a key is explained using drawing 10. Ko is a key used when enciphering data by the public key of a public key system here, Kp is a key used when decoding the data enciphered with the secret key of the public key system, and Kc is a contents key used when decoding the re-enciphered contents data which was described in the 4th example. The encryption communication control section 61 creates the key storing directions having contained own authentication data, the secret key Kp currently held beforehand, and a pair of public key Ko, and transmits this to the key storing card 53 (T1001). In response, the card encryption communication control section 62 of the key storing card 53 attests the digital broadcasting data transfer processor 10 (T1002). And the card encryption communication control section 62 generates session key Ks1 using a random number etc. (T1003), and it enciphers using Ko contained in key storing directions, and it transmits this to the encryption communication control section 61 of the digital broadcasting data transfer processor 10 which is a transmitting agency (T1004). In response, the encryption

communication control section 61 decodes session key Ks1 enciphered using the secret key Kp currently held beforehand, and obtains session key Ks1 (T1005). And random number Ks2 is generated (T1006), this random number Ks2 is enciphered using session key Ks1, and it transmits to the key storing card 53 (T1007). In the card encryption communication control section 62 of the key storing card 53, random number Ks2 enciphered using session key Ks1 is decoded, and random number Ks2 is obtained (T1008). And discernment ID20 [required for encryption of contents] is enciphered using random number Ks2, and it transmits to the encryption communication control section 61 (T1009). Discernment ID enciphered using Ks2 is decoded in the encryption communication control section 61, When obtaining discernment ID (T1010) and decoding content ID and contents from the contents code machine 34, the required license key Kc is obtained (T1011), these are enciphered using session key Ks1, and it transmits to the key storing card 53. And it decrypts using Ks1 by the card encryption communication control section 62 of the key storing card 53, content ID and the license key Kc are obtained, and these are stored in the key storing region 18. Thus, discernment ID required for decoding of contents, content ID, and the license key Kc, It is enciphered, and takes and carries out, and also the data enciphered since session key Ks1 used for these codes and random number Ks2 were generated using a random number etc. turns into data which is different each time, and it becomes difficult to get to know a key only by carrying out the probe of the signal.

[0033]The procedure in the case of obtaining the key which decodes contents (reproduction) using drawing 11 is described. The encryption communication control section 61 creates the key transmission instruction having contained own authentication data, the secret key Kp currently held beforehand, and a pair of public key Ko, and transmits this to the key storing card 53 (T1101). In response, the card encryption communication control section 62 of the key storing card 53 attests the digital broadcasting data transfer processor 10 (T1102). And the card encryption communication control section 62 generates session key Ks1 using a random number etc. (T1103), and it enciphers using Ko contained in key storing directions, and it transmits this to the encryption communication control section 61 of the digital broadcasting data transfer processor 10 which is a transmitting agency (T1104). In response, the encryption communication control section 61 decodes session key Ks1 enciphered using the secret key Kp currently held beforehand, and obtains session key Ks1 (T1105). And random number Ks2 is generated (T1106), this random number Ks2 is enciphered using session key Ks1, and it transmits to the key storing card 53 (T1107). In the card encryption communication control section 62 of the key storing card 53, random number Ks2 enciphered using session key Ks1 is decoded, and random number Ks2 is obtained (T1008). And discernment ID20 and the license key Kc required for decryption of contents are enciphered using random number Ks2, and it transmits to the encryption communication control section 61 (T1109). In the encryption

communication control section 61, discernment ID and the license key Kc which were enciphered using Ks2 are decoded, discernment ID and the license key Kc are obtained (T1110), these discernment ID and license keys Kc are sent to the re-code contents decoder 35, and contents are decrypted. As point ** was carried out also in this case, it becomes difficult to get to know a key only by carrying out the probe of the signal.

[0034]Next, the 7th example is described using drawing 12. It is a contents storing region which stores the contents data which enciphered 57 in drawing 12, 55 is the function of a key storing card to exchange discernment ID and a contents key using the encryption communication explained in the 6th example to a contents storing region the memory storage with a key storing region provided, and 56, They are the card and storing region I/F part for accessing the contents storing region 57, a key storing region, and discernment ID. Operation is explained using these. The case where contents are recorded first is explained. The program enciphered by the tuner 11 is received and it separates into the scramble key Ks enciphered as the contents data enciphered with the eliminator 13 through the contents decoder 12. The separated scramble key Ks which was enciphered sets the scramble key Ks which was decrypted by local CPU15 by IC card 16, and was decrypted by local CPU15 as the contents decoder 12.

[0035]The contents data decoded with the contents decoder 12 is sent to the contents decoder 14 and the contents code machine 36 by the eliminator 13. Contents are decoded by the contents decoder 14, and it outputs to the output unit 30, and can view and listen to contents. In the contents code machine 36, with the random number generated with this and the random number generator 21, discernment ID20 which is the unique identification information for every direction transmitted-and-received-data transmission processing unit is acquired using encryption communication, and it enciphers [are and]. The contents key and content ID which were generated here are written using encryption communication, and it stores in the storing region 18. The contents code machine 36 is stored in the contents area 57 with content ID via a card and a storing region I/F part in the re-enciphered contents data. The re-code contents decoder 37 reads the contents data and content ID which were stored in the contents storing region 57 of the memory storage 55 with a key storing region when decoding and which were enciphered, The contents key and discernment ID corresponding to content ID are read from key storing region 18 and discernment ID20 using encryption communication, respectively, and the enciphered contents data is decoded. And the decrypted contents data is inputted into the contents decoder 14 via the eliminator 13, is outputted with the output unit 30, and can view and listen to contents.

[0036]If contents are re-enciphered, the contents key of the key storing region 18 increases each time, but since the key storing region 18 has only limited capacity, it may fill. It is inconvenient to manage a key storing card by two or more sheets then, and for a user to

manage. However, if composition like drawing 12 is taken, the above problems decrease by deciding the capacity of a key storing region suitably with the capacity of the field which stores contents, and since there are always contents and a key together, need to divide a key and contents, and it is not necessary to manage them, and is convenient for a user. every contents which relates contents data with one contents key for every group of a certain, or divides a contents storing region for every unit of a certain, and is stored there -- related figure **** -- it is also possible to reduce the capacity of a key storing region by things. The contents storing region 57 of drawing 12 can be considered as memory storage with a key storing region because are HDD and a semiconductor memory device, or DVD-RAM and magnetic tape also attach an electrode etc. to the case of media and give a key storing region and discernment ID to it.

[0037]Next, the 8th example is described using drawing 13. It is a contents key used when 69 decodes enciphered content in drawing 13, 68 is a key index corresponding to the contents key 69, 67 is a key storing region which stores two or more contents keys 69 and the pair of the key index 68, and 40 is a key-index code decoder which enciphers or decrypts a key index.

[0038]Operation is explained using these. The case where contents are recorded first is explained. The program enciphered by the tuner 11 is received and it separates into the scramble key Ks enciphered as the contents data enciphered with the eliminator 13 through the contents decoder 12. The separated scramble key Ks which was enciphered sets the scramble key Ks which was decrypted by local CPU15 by IC card 16, and was decrypted by local CPU15 as the contents decoder 12. The contents data decoded with the contents decoder 12 is sent to the contents decoder 14 and the contents code machine 38 by the eliminator 13. Contents are decoded by the contents decoder 14, and it outputs to the output unit 30, and can view and listen to contents. The key index which decides which [of the contents key which has two or more key storing regions 67 in the contents code machine 38 using the random number generated with the random number generator 21] to use is generated, This key index is transmitted to the key storing card 66 using encryption communication, and contents key 69 and discernment ID20 corresponding to the key index 68 is obtained. Contents data is enciphered using the contents key and discernment ID which were acquired here, A key index is enciphered using the specific key which is the key-index code decoder 40, and with the enciphered contents data, it transmits to the main memory 3 via the bus I/F part 23, and, eventually, stores in the memory storage 5 or the external storage 8. In a key-index code decoder. Since it will become the same data if the result enciphered as enciphering with a certain specific key also has the the same key index, if the redundant data of a random number etc. is attached to a key index and it enciphers, a possibility that results will also differ and a key index will be decoded will become low. Next, the case where the

recorded contents are reproduced is explained. The re-enciphered data which was stored in the memory storage 5 is read by CPU1, and is inputted into the re-code contents decoder 39 through the bus I/F part 23 via PCI bus 4. A key index is decoded for the enciphered key index which is stored with contents data at this time with a specific key with the key-index code decoder 40, and a key index is obtained. And a key index is transmitted to a key storing card using encryption communication, and contents key 69 and discernment ID20 corresponding to the key index 68 is obtained. And contents data is decoded with a re-code contents decoder, it inputs into the eliminator 13, the excessive data of content ID etc. is deleted, and it transmits to the contents decoder 14. It is decoded by the contents decoder 14, is sent to the output unit 30, and can view and listen.

[0039]When it enciphers since it is not necessary to add a new contents key to a key storing card, if it has such composition, and it stores contents, even if the number of contents increases, a key storing card does not have a fear of increasing -- a user -- one sheet -- since what is necessary is just to only carry out card management, management of a key becomes easy and is convenient. .Since it is different in a contents key and discernment ID also differs again, even if it is going to reproduce using a different key storing card and the key storing card used at the time of encryption by changing a contents key and discernment ID for every lock management card is the same key index. Since contents data can be decoded, copyright protection becomes possible.

[0040]By decoding the enciphered key which decodes the contents data enciphered in the device which receives broadcast data, and re-enciphering, if this invention is caused like 1 operative condition as explained above. Also in data processing devices, such as PC in which the application which can store the contents data enciphered by memory storage and can perform a file operation operates, Even if protection of the copyright of contents data is possible and the work key kw is changed, the digital broadcasting data transfer processor which can view and listen to contents can be provided. With [the function which decodes the enciphered key which decodes the enciphered contents data, and is re-enciphered] removal or a possible structure, viewing and listening of contents is attained also with another data processing device.

[0041]

[Effect of the Invention]The contents enciphered and transmitted by the composition of this invention are saved, and it becomes possible to reproduce.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a system configuration figure of the information processor of the 1st example of this invention.
[Drawing 2]It is a system configuration figure of the conventional restricted reception system.
[Drawing 3]It is 1 system-configuration figure of the information processor which receives and records digital broadcasting data.
[Drawing 4]It is a system configuration figure of the code machine which re-enciphers the scramble key of the 1st example of this invention.
[Drawing 5]It is a system configuration figure of the information processor of the 2nd example of this invention.
[Drawing 6]The system configuration figure of the information processor of the 3rd example of this invention.
[Drawing 7]The system configuration figure of the information processor of the 4th example of this invention.
[Drawing 8]It is a block diagram showing the 5th example of this invention.
[Drawing 9]It is a sequence diagram for an example of the exchange of data which stores a key using encryption communication to be shown.
[Drawing 10]It is a sequence diagram for an example of an exchange of the data which acquires a key using encryption communication to be shown.
[Drawing 11]It is a block diagram showing the 6th example of this invention.
[Drawing 12]It is a block diagram showing the 7th example of this invention.
[Drawing 13]It is a block diagram showing the 8th example of this invention.
[Description of Notations]
1 [... PCI bus,] ... CPU, 2 ... A bus bridge, 3 ... Main memory, 4 5 [... External storage,] ... Memory storage, 6 ... A display control part, 7 ... CRT, 8 10 ... A digital broadcasting data transfer

processor, 11 ... Tuner, 12 ... A contents decoder, 13 ... An eliminator, 14 ... Contents decoder, 15 [... A key storing region, 19 / ... Ks code machine, 20 / ... Discernment ID, 21 / ... A random number generation, 22 / ... Ks multiplex machine, 23 / ... A bus I/F part, 24 / ... A local bus, 30 / ... Output unit] ... Local CPU, 16 ... An IC card, 17 ... Ks decoder, 18

[Translation done.]

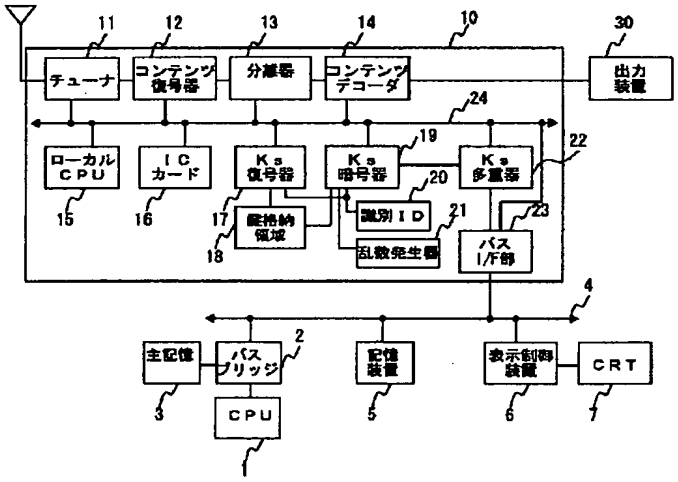
* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

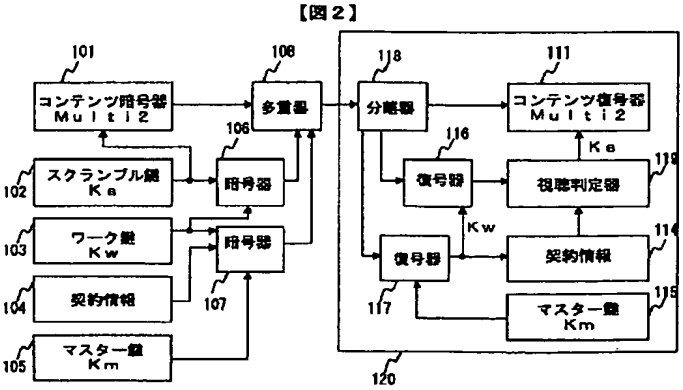
[Drawing 1]

【図１】



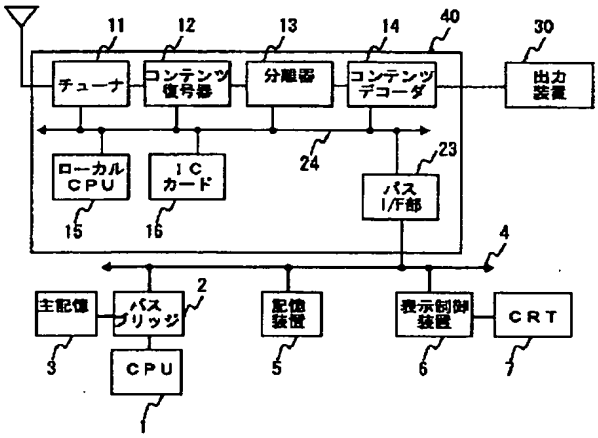
[Drawing 2]

【図２】



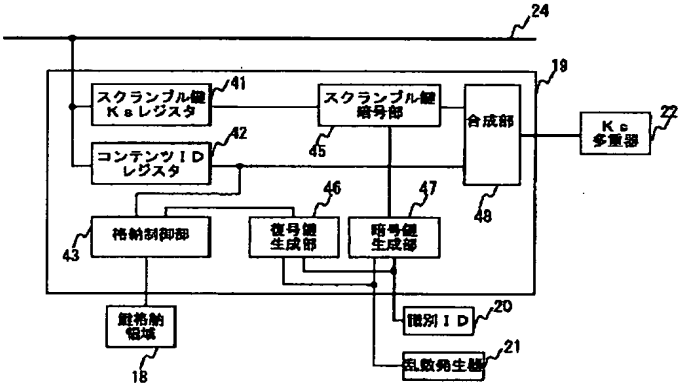
[Drawing 3]

【図３】



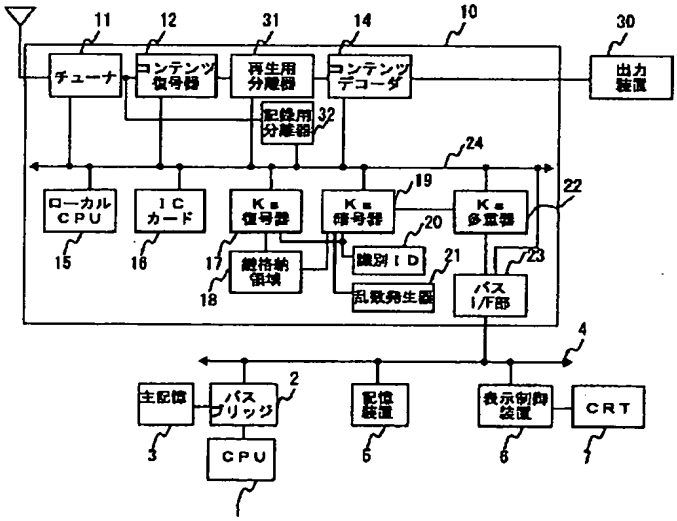
[Drawing 4]

【図４】



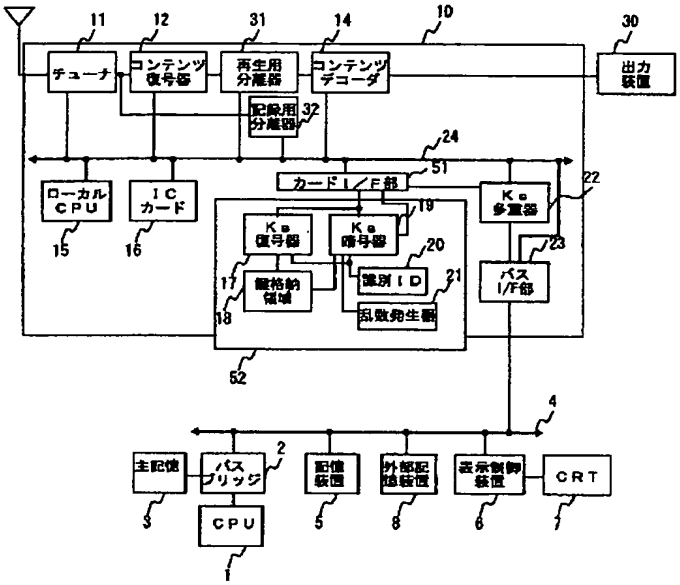
[Drawing 5]

【図５】



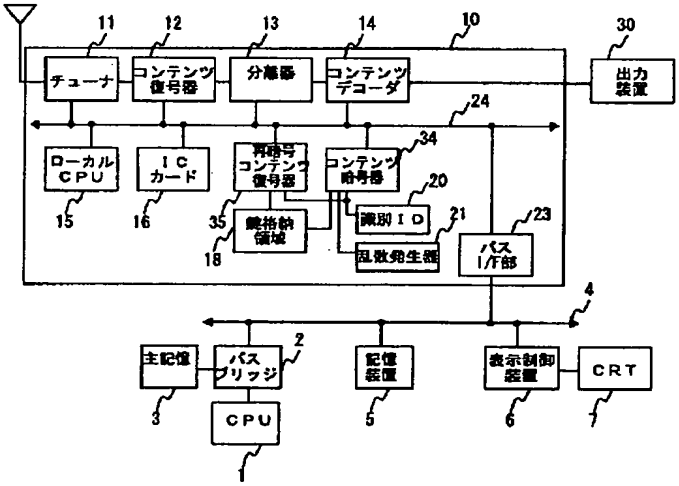
[Drawing 6]

【図６】



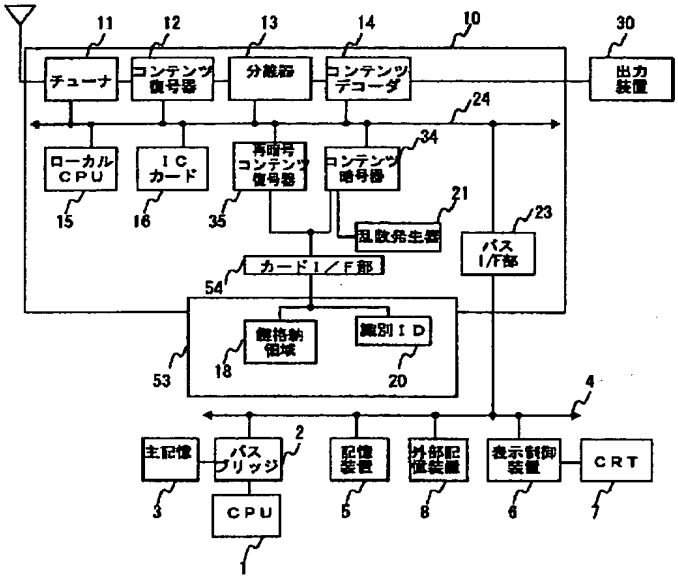
[Drawing 7]

【図７】



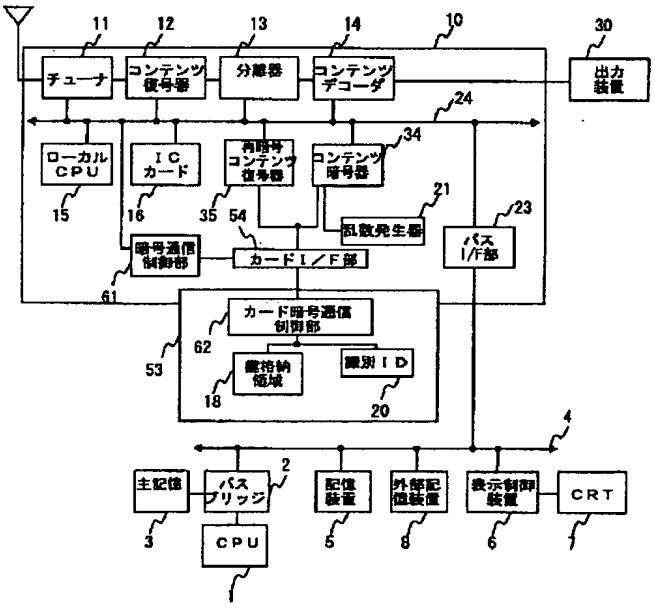
[Drawing 8]

【図８】



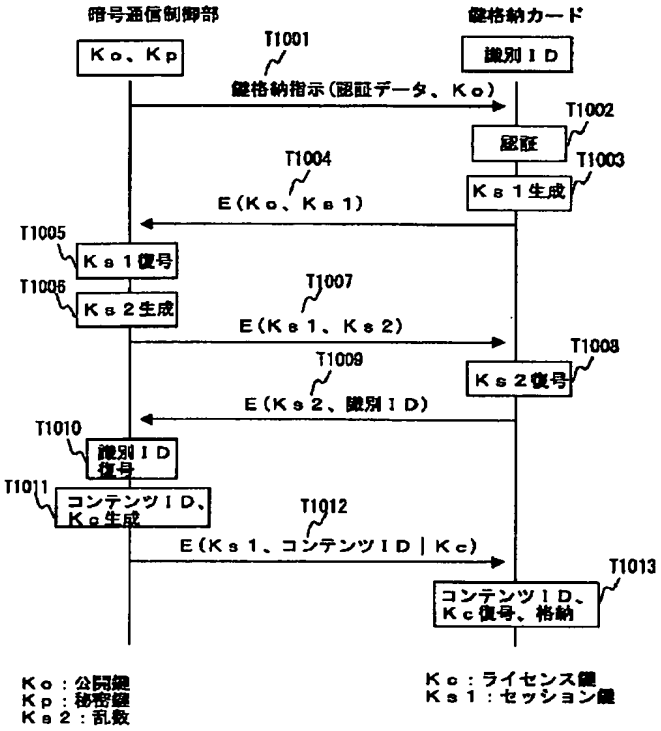
[Drawing 9]

【図９】



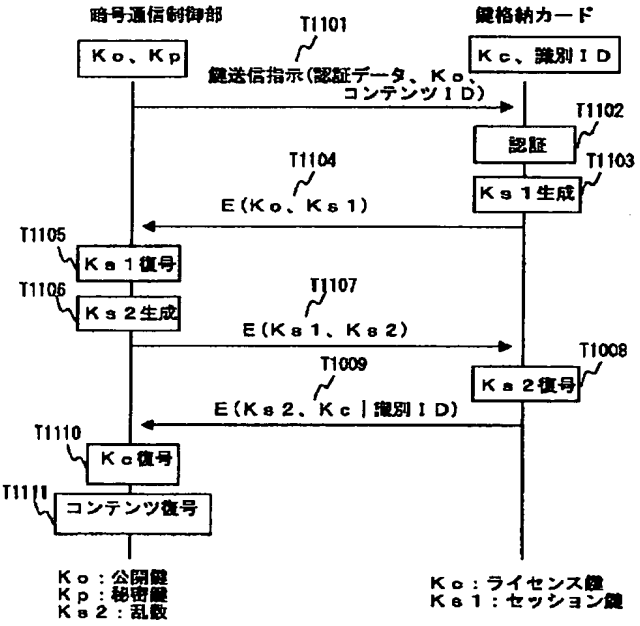
[Drawing 10]

【図１０】



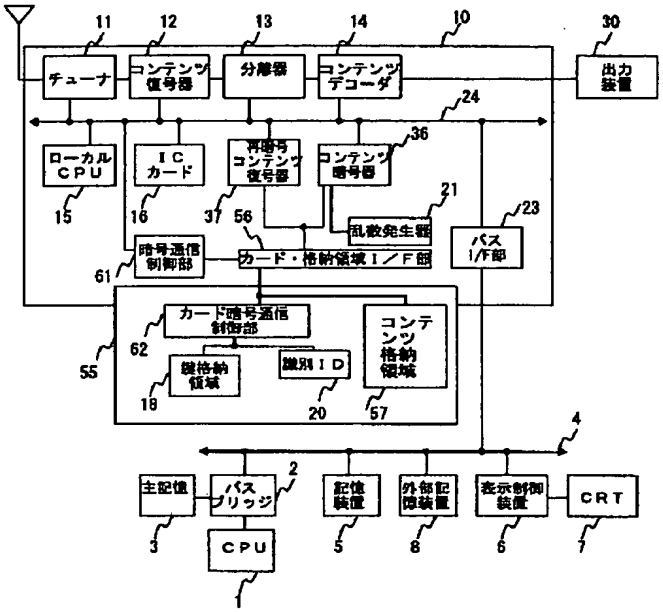
[Drawing 11]

【図１１】



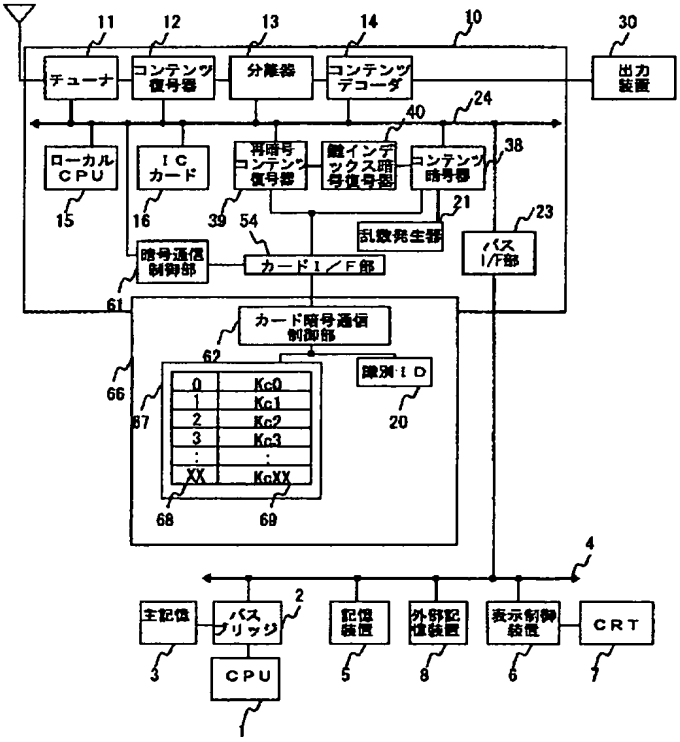
[Drawing 12]

【図１２】



[Drawing 13]

【図１３】



[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CORRECTION OR AMENDMENT

[Kind of official gazette]Printing of amendment by the regulation of 2 of Article 17 of Patent Law

[Section classification] The 3rd classification of the part VII gate
[Publication date]June 23, Heisei 17 (2005.6.23)

[Publication No.]JP,2002-305512,A (P2002-305512A)
[Date of Publication]October 18, Heisei 14 (2002.10.18)
[Application number]Application for patent 2001-91685 (P2001-91685)
[The 7th edition of International Patent Classification]

H04L 9/08

H04H 1/00
[FI]

H04L 9/00 601 A

H04H 1/00 F

H04L 9/00 601 D
[Written amendment]
[Filing date]September 29, Heisei 16 (2004.9.29)
[Amendment 1]
[Document to be Amended]Specification
[Item(s) to be Amended]Claim
[Method of Amendment]Change
[The contents of amendment]
[Claim(s)]
[Claim 1]

It is the enciphered data and said data is a data receiver which receives data decrypted with a data decryption key with which the contents are changed by the passage of time,
a receiver which receives said data enciphered by the 1st encryption key -- and
It has a code machine which is connected with a decoder which decrypts at least one side of said data decryption key enciphered by said data and the 2nd encryption key which were received, and re-enciphers said decrypted data or said data decryption key with a re-enciphering key,
A data receiver being connected with said code machine and memorizing at least one side to a storage among said re-enciphered data and said re-enciphered data decryption key.
[Claim 2]
It is the data receiver according to claim 1,
It has the multiplexing machine connected with said code machine,
Said decoder decrypts said data decryption key,
Said code machine enciphers said decrypted data decryption key,
Said multiplexing machine matches said re-enciphered data decryption key and said received data,
A data receiver, wherein said thing [memorizing said matched data decryption key which was re-enciphered and said data to said storage].
[Claim 3]
It is the data receiver according to claim 2,
A data receiver, wherein said code machine generates a re-decode key which decodes said data decryption key enciphered with the code machine concerned, associates said re-enciphered data decryption key and said decode key of each other and memorizes them to the 2nd storage.
[Claim 4]
It is the data receiver according to claim 2,
It has the 1st eliminator and 2nd eliminator that were connected to said receiver,
Said receiver receives transmit information containing said enciphered data and said enciphered data decryption key,
Said 1st eliminator divides said transmit information into said data and said data decryption key, decrypts said separated data, and transmits to a display,
A data receiver, wherein said 2nd eliminator divides said transmit information into said data and said data decryption key, transmits said separated data decryption key to said decoder and transmits said separated data to said multiplex machine.
[Claim 5]
It is the data receiver according to claim 2,
A data receiver, wherein said re-enciphering key created based on identification information

which identifies the data receiver concerned is used for said code machine.
[Claim 6]
It is the data receiver according to claim 5,
A data receiver, wherein said re-enciphering key based on a random number by which it is generated with a random number generator is used for said code machine.
[Claim 7]
It is the data receiver according to claim 2,
It has an interface unit linked to a processing unit which has said decoder,
A data receiver, wherein said re-enciphering key created based on identification information which identifies said processing unit is used for said code machine.
[Claim 8]
It is the data receiver according to claim 7,
A data receiver, wherein said re-enciphering key based on a random number by which it is further generated with a random number generator is used for said code machine.
[Claim 9]
It is the data receiver according to claim 2,
A data receiver, wherein the data receiver concerned has said storage further.
[Claim 10]
It is the data receiver according to claim 2,
A data receiver connecting the data receiver concerned with said storage via a bus.
[Claim 11]
It is the data receiver according to claim 2,
the 2nd decoder that decrypts said data which decrypted said data decryption key enciphered with said code machine, and was memorized by said storage using said decrypted data decryption key according to an input from a user of the data receiver concerned -- and
A data receiver having an output machine which is connected with said 2nd decoder and outputs said decrypted data.
[Claim 12]
It is the data receiver according to claim 1,
Said decoder decrypts said received data,
Said code machine generates the 2nd decode key for enciphering said decrypted data and decoding said enciphered data,
A data receiver relating said 2nd decode key of each other with the 2nd storage, and memorizing said data enciphered with said code machine to said storage.
[Claim 13]
It is the data receiver according to claim 12,
It has the 1st eliminator and 2nd eliminator that were connected to said receiver,

Said receiver receives transmit information containing said enciphered data and said enciphered data decryption key,
Said 1st eliminator divides said transmit information into said data and said data decryption key, decrypts said separated data, and transmits to a display,
A data receiver, wherein said 2nd eliminator divides said transmit information into said data and said data decryption key and transmits said separated data to said decoder.
[Claim 14]
It is the data receiver according to claim 12,
A data receiver, wherein said re-enciphering key created based on identification information which identifies the data receiver concerned is used for said code machine.
[Claim 15]
It is the data receiver according to claim 14,
A data receiver, wherein said re-enciphering key based on a random number by which it is further generated with a random number generator is used for said code machine.
[Claim 16]
It is the data receiver according to claim 12,
It has an interface unit linked to a processing unit which has said decoder,
A data receiver, wherein said re-enciphering key created based on identification information which identifies said processing unit is used for said code machine.
[Claim 17]
It is the data receiver according to claim 16,
A data receiver, wherein said re-enciphering key based on a random number by which it is further generated with a random number generator is used for said code machine.
[Claim 18]
It is the data receiver according to claim 12,
A data receiver, wherein the data receiver concerned has said storage further.
[Claim 19]
It is the data receiver according to claim 12,
A data receiver connecting the data receiver concerned with said storage via a bus.
[Claim 20]
It is the data receiver according to claim 12,
A data receiver having the 2nd interface unit linked to the 2nd processing unit that has said 2nd storage.
[Claim 21]
It is the data receiver according to claim 12,
the 2nd decoder that decrypts said data memorized by said storage using said 2nd decode key according to an input from a user of the data receiver concerned -- and

A data receiver having an output machine which is connected with said 2nd decoder and outputs said decrypted data.

[Claim 22]

It is the data receiver according to claim 1,

A data receiver, wherein said receiver receives broadcast information which the contents are changed for every said enciphered data which is broadcast from a broadcasting station, and given period, and contains an enciphered data decryption key

[Claim 23]

It is the data receiver according to claim 1,

A data receiver, wherein said 1st encryption key is said 2nd encryption key.

[Claim 24]

It is the enciphered data and said data is a data reproduction apparatus which reproduces data decrypted with a data decryption key with which the contents are changed by the passage of time,

A means which reads from a storage said data decryption key enciphered with said data enciphered with the 1st encryption key, and the 2nd encryption key,

A means to decrypt said data decryption key,

a means to decrypt read data using said decoded data decryption key -- and

A data reproduction apparatus having a means to output said decrypted data.

[Claim 25]

It is the data receiver according to claim 3, and is a pan,

A data receiver having the 2nd interface unit linked to the 2nd processing unit that has said 2nd storage.

[Claim 26]

It is the data receiver according to claim 25,

A data receiver, wherein said 2nd interface unit transmits and receives said re-decode key stored in said 2nd storage using encryption communication.

[Claim 27]

It is the data receiver according to claim 20,

A data receiver, wherein said 2nd interface unit transmits and receives said re-decode key stored in said 2nd storage using encryption communication.

[Claim 28]

It is the data receiver according to claim 1,

It is connected with said code machine and has a key storage which memorizes one or more keys,

At least one of keys memorized by said key storage is used for said code machine, At least one side is re-enciphered among said decrypted data and said decrypted data decryption key,

At least one side is associated among a key used for said re-encryption, said said re-enciphered data, and said re-enciphered data decryption key, A data receiver storing at least one side in said storage among said said re-enciphered data and said re-enciphered data decryption key.

[Claim 29]

It is the data receiver according to claim 1,

A data receiver, wherein said code machine re-enciphers said data decrypted at least.

[Translation done.]